WFS709TP ProSafe Smart Wireless Switch Software Administration Manual

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10265-01
June 2007

Technical Support

Please refer to the support information card that shipped with your product. By registering your product at *http://www.netgear.com/register*, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, INC. Support Information

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card.

E-mail: support@netgear.com

North American NETGEAR

http://www.netgear.com

Trademarks

NETGEAR, the NETGEAR logo, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc. Other brand and product names are registered trademarks or trademarks of their respective holders. Portions of this document are copyright Intoto, Inc.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Certificate of the Manufacturer/Importer

It is hereby certified that the WFS709TP ProSafe Smart Wireless Switch has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß dasWFS709TP ProSafe Smart Wireless Switch gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end user to comply with the applicable requirements may result in unlawful operation and adverse action against the end user by the applicable National regulatory authority.

NOTE: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

United States

FCC Class A

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This product is UL Listed (UL60950).

Canada

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le ministère des Communications.

This product complies with CAN/CSA C22.2 No 60950 standards.

Europe

The WFS709TP ProSafe Smart Wireless Switch is compliant with the following EU Council Directives: 89/336/EEC and LVD 73/23/EEC. Compliance is verified by testing to the following standards: EN55022 Class A, EN55024, and EN60950.

	**Warning:** This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures

Japan

This equipment is in the Class A category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines that are aimed at preventing radio interference in commercial and/or industrial areas. Consequently, when this equipment is used in a residential area or in an adjacent area thereto, radio interference may be caused to equipment such as radios and TV receivers.

VCCI - Class A

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korea

Class A

주의 A급 기기 이 기기는 업무용으로 전자파 적합 등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Australia/New Zealand

This product complies with AS/NZS CISPR 22 Class A standards.

Rest of World

This product complies with CISPR 22 Class A standards

Lithium Battery Safety Notice

This product contains a lithium battery which is replaceable only by a trained technician

Caution: The lithium battery may explode if it is incorrectly replaced. A trained technician should replace the battery with the same or equivalent type battery recommended by the manufacturer. Dispose of used batteries according to the manufacturer’s instructions

European Union RoHS

Netgear products comply with the EU Restriction of Hazardous Substances Directive 2002/95/EC (RoHS). EU RoHS restricts the use of specific hazardous materials in the manufacture of electrical and electronic equipment. Specifically, restricted materials under the RoHS Directive are Lead (including Solder used in printed circuit assemblies), Cadmium, Mercury, Hexavalent Chromium, and Bromine compounds of PBB and PBDE. Some Netgear products are subject to the exemptions listed in RoHS Directive Annex 7 (Lead in solder used in printed circuit assemblies). Products and packaging will be marked with the "RoHS" label shown at the left indicating conformance to this Directive.

China RoHS

Netgear products comply with China environmental declaration requirements and are labeled with the "EFUP 50" label shown at the left.

有毒有害物质声明
Hazardous Materials Declaration

部件名称 (Parts)	有毒有害物质或元素 (Hazardous Substances)					
	铅 Lead (Pb)	汞 Mercury (Hg)	镉 Cadmium (Cd)	六价铬 Chromium VI Compounds (Cr^{6+})	多溴联苯 Polybrominated Biphenyls (PBB)	多溴二苯醚 Polybrominated Diphenyl Ether (PBDE)
电路板 PCA Board	X	O	O	O	O	O
机械组件 Mechanical Subassembly	X	O	O	O	O	O

O: 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T11363-2006标准规定的限量要求以下。
This component does not contain this hazardous substance above the maximum concentration values in homogeneous materials specified in the SJ/T11363-2006 Industry Standard.

X: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T11363-2006标准规定的限量要求。
This component does contain this hazardous substance above the maximum concentration values in homogeneous materials specified in the SJ/T11363-2006 Industry Standard.

对销售之日的所售产品，本表显示，供应链的电子信息产品可能包含这些物质。
This table shows where these substances may be found in the supply chain of electronic information products, as of the date of sale of the enclosed product.

此标志为针对所涉及产品的环保使用期标志。
某些零部件会有一个不同的环保使用期(例如，电池单元模块)贴在其产品上。
此环保使用期限只适用于产品是在产品手册中所规定的条件下工作。
The Environment- Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here. The Environment- Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.

Part Number: 0510303-01

Product and Publication Details

Model Number:	WFS709TP
Publication Date:	June 2007
Product Family:	Wireless
Product Name:	WFS709TP ProSafe Smart Wireless Switch
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10265-01
Publication Version Number:	1.0

Contents

About This Manual

The *WFS709TP ProSafe™ Smart Wireless Switch Software Administration Manual* describes how to deploy and configure the WFS709TP ProSafe Smart Wireless Switch. It also includes instructions for and examples of commonly used wireless LAN (WLAN) switch configurations such as Virtual Private Networks (VPNs) and redundancy.

Conventions, Formats, and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions.** This manual uses the following typographical conventions:

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italic	URL links

- **Formats.** This manual uses the following formats to highlight special messages:

	**Note:** This format is used to highlight information of importance or special interest.

	**Tip:** This format is used to highlight a procedure that will save time or resources.

	**Warning:** Ignoring this type of note may result in a malfunction or damage to the equipment.

	**Danger:** This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope.** This manual is written for the WFS709TP according to these specifications:

Product Version	WFS709TP ProSafe Smart Wireless Switch
Manual Publication Date	June 2007

For more information about network amd wireless technologies, see the links to the NETGEAR website in Appendix D, "Related Documents".

	**Note:** Product updates are available on the NETGEAR, Inc. website at *http://www.netgear.com/support.*

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons,  and  , for browsing forwards or backwards through the manual one page at a time
- A  button that displays the table of contents and an  button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual
- A  button to access the full NETGEAR, Inc. online knowledge base for the product model
- Links to PDF versions of the full manual and individual chapters

How to Print this Manual

To print this manual, choose one of the following options:

- **Printing a Page from HTML**. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.

- **Printing from PDF**. Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe website at *http://www.adobe.com*.
  - **Printing a PDF Chapter.** Use the *PDF of This Chapter* link at the top left of any page.
    - Click the *PDF of This Chapter* link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
    - Click the print icon in the upper left of your browser window.
  - **Printing a PDF version of the Complete Manual**. Use the *Complete PDF Manual* link at the top left of any page.
    - Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
    - Click the print icon in the upper left of your browser window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

Part Number	Version Number	Date	Description
202-10265-01	1.0	June 2007	Initial NETGEAR release.

Chapter 1
Overview of the WFS709TP

The WFS709TP ProSafe Smart Wireless Switch is a full-featured wireless switch that centrally manages NETGEAR Light access points, delivering integrated wireless mobility, security, and converged services for both wired and wireless users.

This chapter describes the components and features of the WFS709TP ProSafe Smart Wireless Switch, in the following topics:

WFS709TP System Components

The WFS709TP ProSafe Smart Wireless Switch system consists of the following components:

The following sections describe each of these components.

NETGEAR ProSafe Access Points

The NETGEAR ProSafe WAGL102 and ProSafe WGL102 access points (APs) are designed for the WFS709TP, and provide the best features and easiest integration. Several other NETGEAR access point products can also be repurposed to work with the WFS709TP. Refer to the NETGEAR support site for a list of which NETGEAR APs can be repurposed, and for instructions on how to do so.

An AP broadcasts its configured service set identifier (SSID), which corresponds to a specific wireless local area network (WLAN). Wireless clients discover APs by listening for broadcast beacons or by sending active probes to search for APs with a specific SSID.

You can connect an AP to a WFS709TP either directly with an Ethernet cable or remotely through an IP network. Figure 1-1 shows two APs connected to an WFS709TP. One AP is connected to a switch in the wiring closet that is connected to a router in the data center where the WFS709TP is located. The Ethernet port on the other AP is cabled directly to a port on the WFS709TP.

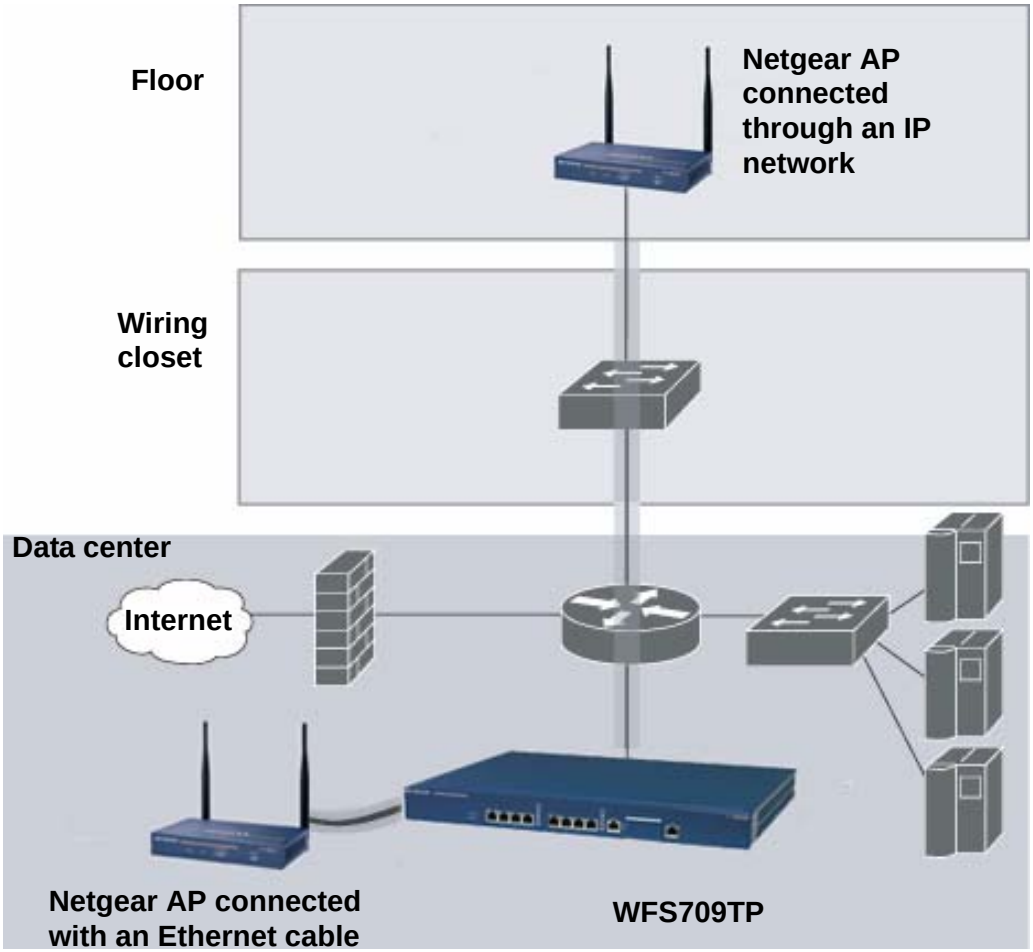

Figure 1-1

Access points used with the WFS709TP are Light APs, which means their primary function is to receive and transmit wireless RF signals; other WLAN processing is left to the WFS709TP itself. When powered on, an AP locates its host switch through a variety of methods, including the Aruba Discovery Protocol (ADP), Domain Name Service (DNS), or D ynamic Host Configuration

Protocol (DHCP). Once an AP locates its host switch, it automatically builds a secure Generic Routing Encapsulation (GRE) tunnel to it (Figure 1-2). The AP then downloads its firmware and configuration from the switch through the tunnel.

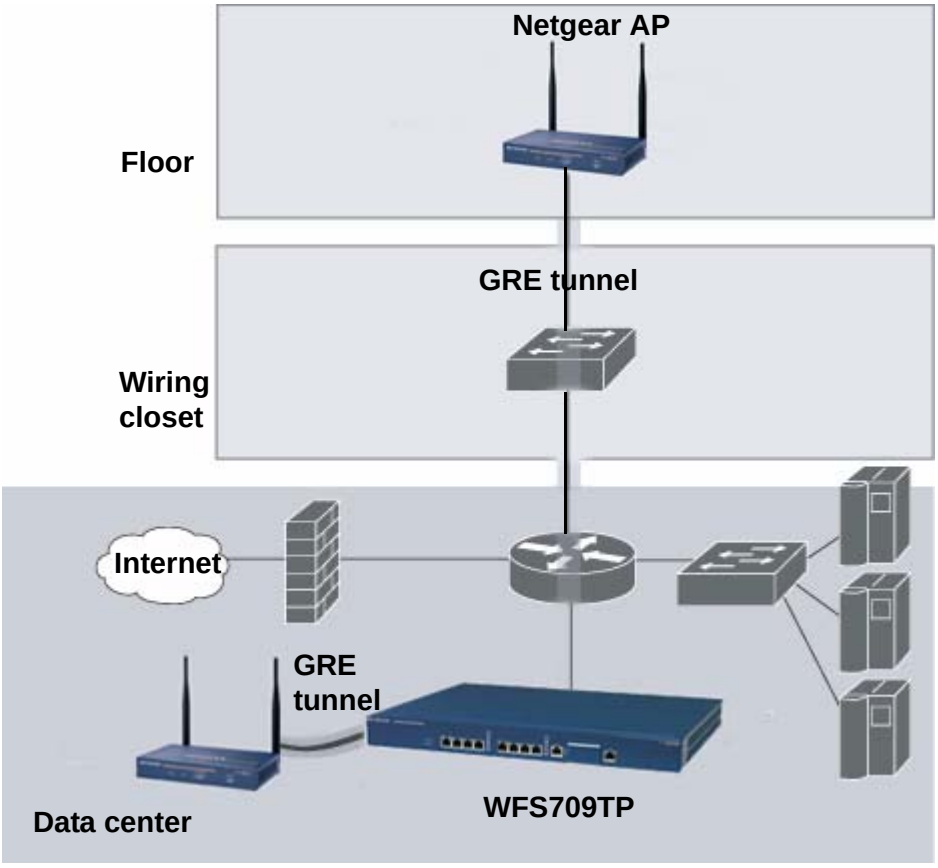

Figure 1-2

Client traffic received by the AP is immediately sent through the tunnel to the host WFS709TP (Figure 1-3), which performs packet processing such as encryption and decryption, authentication, and policy enforcement

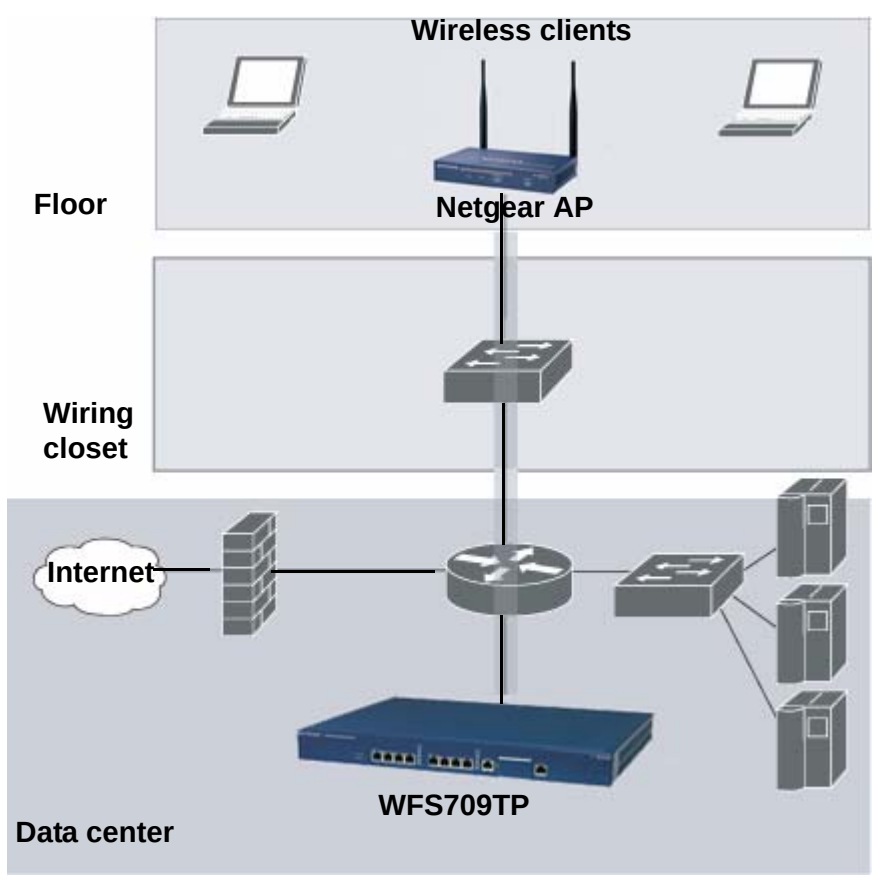

Figure 1-3

Automatic RF Channel and Power Settings

IntelliFi RF Management (IRM) is a radio frequency (RF) resource allocation algorithm that you can enable and configure in the WFS709TP system. When IRM is enabled, each AP can determine the optimum channel selection and transmitter power setting to minimize interference and maximize coverage and throughput. The APs scan for better channels at periodic intervals and report information to the WFS709TP. The WFS709TP analyzes reports from all APs and coordinates changes, resulting in a higher-performance RF environment.

If an AP fails for any reason, the system's self-healing mechanism automatically ensures coverage for wireless users. The WFS709TP detects the failed AP and instructs neighboring APs to increase power levels to compensate.

You can also enable WFS709TPs to detect coverage holes, or areas where a good RF signal is not adequately reaching wireless clients.

RF Monitoring

An AP can function as either a dedicated or shared Air Monitor (AM) to monitor the RF spectrum to detect intrusions, denial of service (DoS) attacks, and other vulnerabilities. A *dedicated* AM performs monitoring functions exclusively and does not service wireless clients or advertise SSIDs. A *shared* AM performs monitoring functions in addition to servicing wireless clients.

Every AP automatically monitors the channel on which it services wireless clients. You can configure the AP to perform off-channel scanning, where the AP spends brief time intervals scanning other channels. However, the more clients an AP services, the less time it has to perform off-channel scanning. If air monitoring functions are critical to your network, designate a few APs as dedicated AMs.

You can configure dedicated AMs to perform the following functions:

- Detect, locate, and disable rogue APs (APs that are not authorized or sanctioned by network administrators)
- Detect and disable ad-hoc networks
- Detect and disable honeypot APs
- Detect wireless bridges
- Capture remote packets

If you only need air monitoring functions periodically, you can configure APs to operate temporarily as AMs. You can also configure dedicated AMs to automatically convert into APs if an AP failure occurs or when there is a high level of traffic on the network.

WFS709TP ProSafe Switches

All APs are connected either directly or remotely through an IP network to the WFS709TP ProSafe Smart Wireless Switch. The WFS709TP is an enterprise-class switch that bridges wireless client traffic to and from traditional wired networks and performs high-speed Layer 2 or Layer 3 packet forwarding between Ethernet ports. While APs provide radio services only, the WFS709TP performs upper-layer media access control (MAC) processing, such as encryption and authentication, as well as centralized configuration and management of SSIDs and RF characteristics for the APs. This allows you to deploy APs with little or no physical change to an existing wired infrastructure.

WFS709TP switches provide 10/100 Mbps Fast Ethernet, IEEE 802.3af-compliant ports that can provide Power over Ethernet (PoE) to directly connected APs. When you connect a PoE-capable port on the WFS709TP to a PoE-compatible device such as an AP, the port automatically detects the device and provides operating power through the connected Ethernet cable. This allows APs to be installed in areas where electrical outlets are unavailable, undesirable, or not permitted, such as in the plenum or in air-handling spaces.

At least one WFS709TP is the *master* switch while non-master switches are referred to as *local* switches (Figure 1-4). A master WFS709TP offers a single point of configuration that is automatically replicated from the master to local WFS709TPs throughout the network.

Local WFS709TPs offer local points of traffic aggregation and management for APs and services. A local WFS709TP can perform any supported function (for example, WLAN management or policy enforcement). However, these services are always configured on the master WFS709TP and are "pushed" to specified local WFS709TPs.

An AP obtains its firmware image and configuration from a master switch; it can also be instructed by a master switch to obtain its software from a local switch.

Note: For information about configuring the switch for master or local status, see the "Run the Initial Setup" on page 2-6.

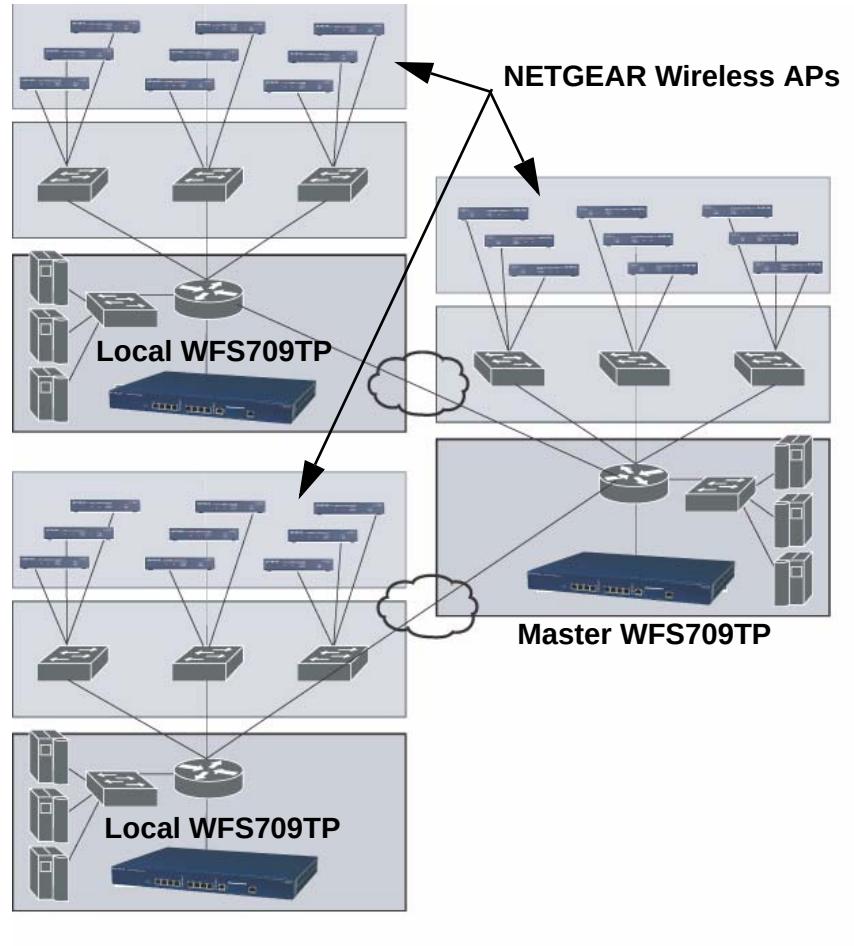

Figure 1-4

Your network can include one master WFS709TP, one or more backup master WFS709TPs, and any number of local WFS709TPs. Master WFS709TPs do not share information with each other, so APs that share roaming tables, security policies, and other configurations should be managed by the same master WFS709TP.

WFS709TP Software

The WFS709TP ProSafe Smart Wireless Switch software is a suite of mobility applications that runs on all WFS709TPs and allows you to configure and manage the wireless and mobile user environment.

The base configuration software includes the following functions:

- Centralized configuration and management of APs
- Wireless client authentication to an external authentication server or to the WFS709TP's local database
- Encryption
- Mobility with fast roaming
- RF management and analysis tools

Basic WLAN Configuration

You have a wide variety of options for authentication, encryption, access management, and user rights when you configure a WLAN in a WFS709TP system. However, you must configure the following basic elements:

- An SSID that uniquely identifies the WLAN
- Layer 2 authentication to protect against unauthorized access to the WLAN
- Layer 2 encryption to ensure the privacy and confidentiality of the data transmitted to and from the network
- A user role and virtual local area network (VLAN) for the authenticated client

This section describes authentication, encryption, and VLAN configuration in the WFS709TP system.

Authentication

A user must authenticate to the system in order to access WLAN resources. There are several types of Layer 2 security mechanisms allowed by the IEEE 802.11 standard that you can employ, including those that require an external RADIUS authentication server.

- **None** (also called open system authentication). This is the default authentication protocol. The client's identity, in the form of the Media Access Control (MAC) address of the wireless adapter in the wireless client, is passed to the WFS709TP. Essentially, any client requesting access to the WLAN is authenticated.

- IEEE 802.1x. The IEEE 802.1x authentication standard allows for the use of keys that are dynamically generated on a per-user basic (as opposed to a static key that is the same on all devices in the network).

	**Note:** The 802.1x standard requires the use of a RADIUS authentication server. Most Lightweight Directory Access Protocol (LDAP) servers do not support 802.1x.

With 802.1x authentication, a *supplicant* is the wireless client that wants to gain access to the network and the device that communicates with both the supplicant and the authentication server is the *authenticator*. In this system, the WFS709TP is the 802.1x authenticator, relaying authentication requests between the authentication server and the supplicant.

	**Note:** During the authentication process, the supplicant (the wireless client) and the RADIUS authentication server negotiate the type of Extensible Authentication Protocol (EAP) they will use for the authentication transaction. The EAP type is completely transparent to the WFS709TP and has no impact on its configuration.

- **Wi-Fi Protected Access (WPA).** WPA implements most of the IEEE 802.11i standard. It is designed for use with an 802.1x authentication server (the Wi-Fi Alliance refers to this mode as WPA-Enterprise). WPA uses the Temporal Key Integrity Protocol (TKIP) to dynamically change keys and RC4 stream cipher to encrypt data.
- **WPA in pre-shared key (PSK) mode (WPA-PSK).** With WPA-PSK, all clients use the same key (the Wi-Fi Alliance refers to this mode as WPA-Personal).

	**Note:** In PSK mode, users must enter a passphrase 8–63 characters in length to access the network. PSK is intended for home and small office networks where operating an 802.1x authentication server is not practical

- **WPA2.** WPA2 implements the full IEEE 802.11i standard. In addition to WPA features, WPA2 provides Counter Mode with Cipher Blocking Chaining Message Authentication Code Protocol (CCMP) for encryption that uses the Advanced Encryption Standard (AES) algorithm. The Wi-Fi Alliance refers to this mode as WPA2-Enterprise.
- **WPA2-PSK.** WPA2-PSK is WPA2 used in PSK mode, where all clients use the same key. The Wi-Fi Alliance refers to this mode as WPA2-Personal.

Encryption

The Layer 2 encryption option you can select depends upon the authentication method chosen. Table 1-1 lists the authentication methods available, with their corresponding encryption options.

Table 1-1. Encryption Options by Authentication Method

Authentication Method	Encryption Option
None	Null or Static WEP
802.1x	Dynamic WEP
WPA or WPA-PSK only	TKIP
WPA2 or WPA2-PSK only	AES
Combination of WPA or WPA-PSK and WPA2 or WPA2-PSK	Mixed TKIP/AES

You can configure the following data encryption options for the WLAN:

- **Null.** No encryption is used and packets passing between the wireless client and WFS709TP are in clear text.
- **Wired Equivalent Protocol (WEP).** Defined by the original IEEE 802.11 standard, WEP uses the RC4 stream cipher with 40-bit and 128-bit encryption keys. The management and distribution of WEP keys is performed outside of the 802.11 protocol. There are two forms of WEP keys:
  - *Static WEP* requires you to manually enter the key for each client and on the WFS709TP.
  - *Dynamic WEP* allows the keys to be automatically derived for each client for a specific authentication method during the authentication process. Dynamic WEP requires 802.1x authentication.
- **Temporal Key Integrity Protocol (TKIP).** TKIP ensures that the encryption key is changed for every data packet. You specify TKIP encryption for WPA and WPA-PSK authentication.
- **Advanced Encryption Standard (AES).** AES is an encryption cipher that uses the Counter-mode CBC-MAC (Cipher Block Chaining-Message Authentication Code) Protocol (CCMP) mandated by the IEEE 802.11i standard. AES-CCMP is specifically designed for IEEE 802.11 encryption and encrypts parts of the 802.11 MAC headers as well as the data payload. You can specify AES-CCMP encryption with WPA2 or WPA2-PSK authentication.
- **Mixed TKIP/AES-CCM.** This option allows the WFS709TP to use TKIP encryption with WPA or WPA-PSK clients and use AES encryption with WPA2 or WPA2-PSK clients. Mixed TKIP/AES-CCM allows you to deploy the system in environments containing existing WLANs that use different authentication and encryption methods.

VLAN

Each authenticated user is placed into a VLAN, which determines the user's DHCP server, IP address, and Layer 2 connection. While you could place all authenticated wireless users into a single VLAN, the system allows you to group wireless users into separate VLANs. This enables you to differentiate groups of wireless users and their access to network resources. For example, you might place authorized employee users into one VLAN and itinerant users, such as contractors or guests, into a separate VLAN.

Note: You create the VLANs for wireless users only on the WFS709TP. You do not need to create the VLANs anywhere else on your network. Because wireless clients are tunneled to the WFS709TP, it appears to the rest of the network as if the clients were directly connected to the WFS709TP.

For example, in the topology shown in Figure 1-5, authenticated wireless users are placed on VLAN 20. You configure VLAN 20 only on the WFS709TP; you do not need to configure VLAN 20 on any other device in the network.

Note: To allow data to be routed to VLAN 20, you must configure a static route to VLAN 20 on an upstream router in the wired network

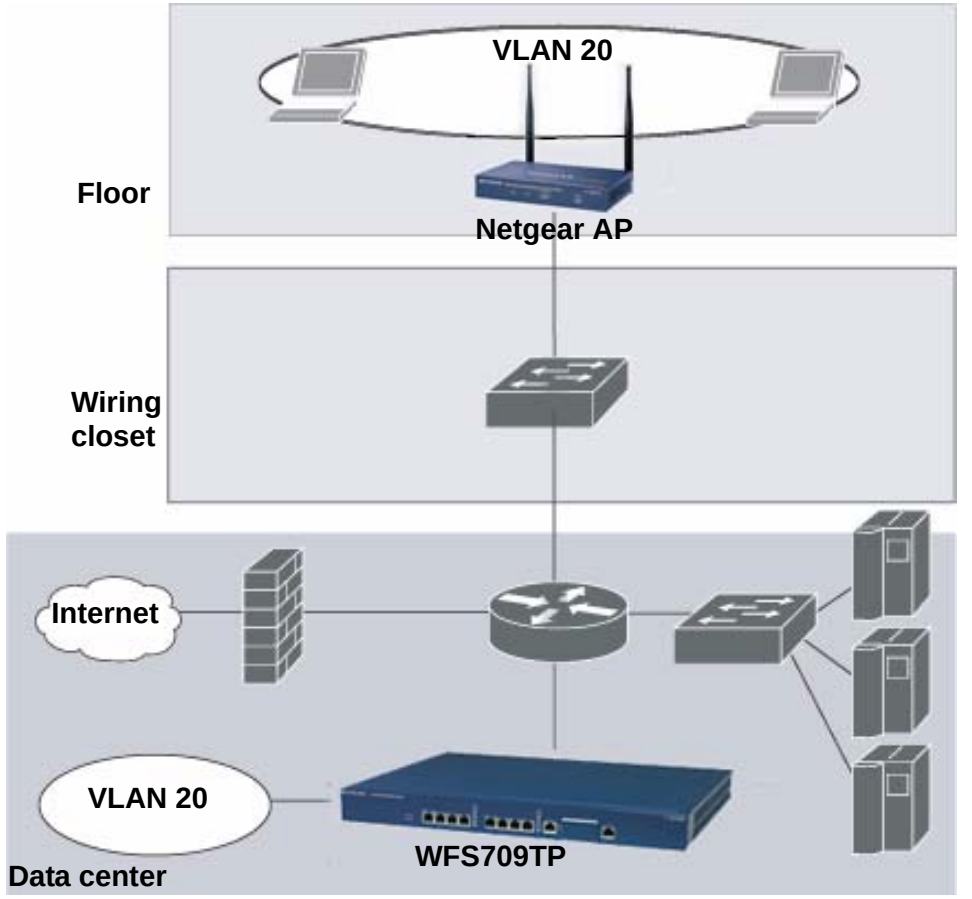

Figure 1-5

A user is assigned to a VLAN by one of several methods, and there is an order of precedence to these methods.The methods for assignment of VLANs are (from lowest to highest precedence):

1. The VLAN is configured for the AP location.
2. The VLAN is derived from rules based on user attributes SSID, BSSID (Basic Service Set Identifier), user MAC, location, and encryption type. Within the set of possible user-derivation rules, a rule that derives a specific VLAN takes precedence over a rule that derives a user role that may have a VLAN configured for it.
3. The VLAN is configured for a default role for an authentication method, such as 802.1x or VPN.

4. The VLAN is derived from attributes returned by the authentication server (server-derived rule). Within a set of server-derived rules, a rule that derives a specific VLAN takes precedence over a rule that derives a user role that may have a VLAN configured for it.
5. The VLAN is derived from Microsoft Tunnel attributes (Tunnel-Type, Tunnel Medium Type, and Tunnel Private Group ID). All three attributes must be present. This does not require any server-derived rule.
6. The VLAN is derived from NETGEAR vendor-specific attributes (VSAs) for RADIUS server authentication. This does not require any server-derived rule.

   If a NETGEAR VSA is present, it overrides any previous VLAN assignment.

Wireless Client Access to the WLAN

Wireless clients communicate through a WLAN with the wired network and other wireless clients in a WFS709TP system. There are two phases to the process by which a wireless client gains access to a WLAN:

1. *Association* of the radio network interface card (NIC) in the PC with an AP, as described by the IEEE 802.11 standard. This association allows data link (Layer 2) connectivity.
2. *Authentication* of the client/user before network access is allowed.

Association

APs send out beacons that contain the SSIDs of specific WLANs; the user can select the network they want to join. Wireless clients can also send out probes to locate a WLAN within range or to locate a specific SSID, and APs within range of the client respond. Along with the SSID, an AP also sends out the following information:

- Data rates supported by the WLAN. Clients can determine which WLAN to associate with based on the supported data rate.
- WLAN requirements for the client. For example, clients may need to use TKIP for encrypting data transmitted on the WLAN.

The client determines which AP is best for connecting to the WLAN and attempts to associate with it. During the association exchange, the client and WFS709TP negotiate the data rate, authentication method, and other options.

Note: Because an AP connected to a WFS709TP is a Thin AP, all wireless traffic it receives is immediately sent through a GRE tunnel to the WFS709TP. The WFS709TP responds to client requests and communicates with an authentication server on behalf of the client. Therefore, the client authentication and association processes occur between the wireless client and the WFS709TP.

Authentication

Authentication provides a way to identify a user and provide appropriate access to the network for that user. One or more authentication methods may be used, ranging from secure authentication methods such as 802.1x and captive portal to less secure methods such as MAC address authentication.

802.1x Authentication

802.1x is an IEEE standard used for authenticating clients on any IEEE 802 network. It is an open authentication framework, allowing multiple authentication protocols to operate within the framework. 802.1x operates as a Layer 2 protocol. Successful 802.1x authentication must complete before any higher-layer communication with the network, such as a DHCP exchange to obtain an IP address, is allowed.

802.1x is key-generating, which means that the output of the authentication process can be used to assign dynamic per-user encryption keys. While the configuration of 802.1x authentication on the WFS709TP is fairly simple, 802.1x can require significant work in configuring an external authentication server and wireless client devices.

Captive Portal

Captive Portal allows a wireless client to authenticate using a web-based portal. Captive portals are typically used in public access wireless hotspots or for hotel in-room Internet access. After a user associates to the wireless network, their device is assigned an IP address. The user must start a web browser and pass an authentication check before access to the network is granted.

Captive portal authentication is the simplest form of authentication to use and requires no software installation or configuration on the client. The username/password exchange is encrypted using standard SSL encryption. However, portal authentication does not provide any form of encryption

beyond the authentication process; to ensure privacy of user data, some form of link-layer encryption (such as WEP or WPA-PSK) should be used when sensitive data will be sent over the wireless network.

MAC Address Authentication

MAC address authentication is the process of examining the media access control (MAC) address of an associated device, comparing it to an internal or RADIUS database, and changing the user role to an authenticated state. MAC address authentication is not a secure form of authentication, as the MAC address of a network interface card (NIC) can be changed in software. MAC address authentication is useful for devices that cannot support a more secure form of authentication, such as barcode scanners, voice handsets, or manufacturing instrumentation sensors.

User roles mapped to MAC address authentication should be linked to restrictive policies to permit only the minimum required communication. Whenever possible, WEP encryption should also be employed to prevent unauthorized devices from joining the network.

Client Mobility and AP Association

When a wireless client associates with an AP, it retains the association for as long as possible. Generally, a wireless client only drops the association if the number of errors in data transmission is too high or the signal strength is too weak.

When a wireless client roams from one AP to another, the WFS709TP can automatically maintain the client's authentication and state information. Clients do not need to reauthenticate or reassociate; the client only changes the radio that it uses. A client roaming between APs that are connected to the same WFS709TP maintains its original IP address and existing IP sessions.

You can also enable client mobility on all switches in a master WFS709TP's hierarchy. This allows clients to roam between APs that are connected to different switches without needing to reauthenticate or obtain a new IP address. When a client associates with an AP, the client information is sent to the master WFS709TP. The master WFS709TP pushes out the client information to all local switches in its hierarchy. If the client roams to an AP connected to a different switch, the new switch recognizes the client and tunnels the client traffic back to the original switch.

Configuring and Managing the WFS709TP

The browser interface allows you to configure and manage WFS709TPs. The browser interface is accessible through a standard web browser from a remote management console or workstation. Before you can use the management interface from a remote console or workstation, you must configure the WFS709TP with an IP address and default gateway and connect it to your network. See Chapter 2, “Deploying a Basic WFS709TP System” for more information.

Note: In this manual, the instructions for reaching a specific browser interface page are shortened to specify the sequence of tab or page selections; for example, “Navigate to the Configuration > Basic > Network > VLAN page.”

All WFS709TPs have a serial port for connecting to a local console, and a 10/100 Mbps Fast Ethernet port for out-of-band management. Refer to the document *WFS709TP ProSafe Smart Wireless Switch Hardware Installation Guide* for more information about the switch’s ports.

Note: You can find the *WFS709TP ProSafe Smart Wireless Switch Hardware Installation Guide* in PDF form on the WFS709TP *Resource CD*. It is also available from the NETGEAR support site.

To use the browser interface, enter the IP address of the WFS709TP in a web browser.

Note: The WFS709TP browser interface requires Internet Explorer 6.0 or higher. Other browsers may work, but have limited functionality and are therefore not supported.

When you connect to the WFS709TP using the browser interface, the system displays the login page (Figure 1-6). Log in using the administrator user account. The password does not display.

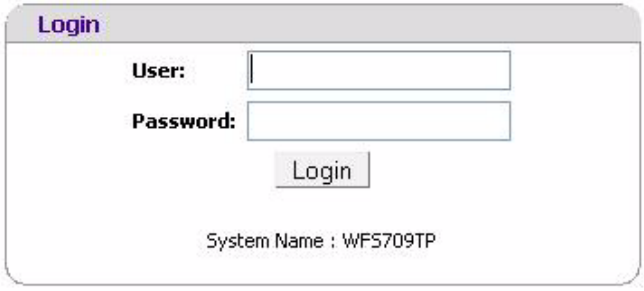

Figure 1-6

When you are logged in, the browser window shows the default Monitor Summary page (Figure 1-7).

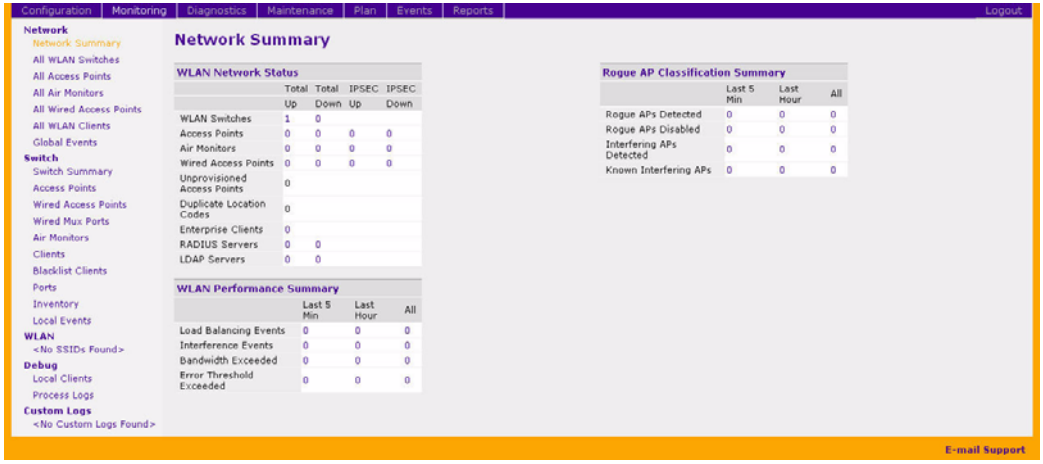

Figure 1-7

The following features are present in all browser interface pages:

- Tabs at the top of the page allow you to select tools available in the browser interface. Click on a tab to select the tool.

- When you select a tab, the tool and its available pages appear in the navigation pane. You can navigate to any of the listed pages by clicking on the page name.

> **Note:** Some of the items in the listed pages are merely headings for their subpages and cannot be selected. Selectable pages become highlighted when you place the cursor over them. Non-selectable items do not react.

- The name of the currently selected page is highlighted in the page tree.
- The main page display area displays all the information and/or input fields relevant to the current page of the current tool.
- The Logout button at the top right corner of the page allows you to end your browser interface session.

Tools

The tool bar at the top of the browser window contains tabs for the various tools available. Click on the tab to select the tool. Table 1-2 lists the tools that are available in the browser interface.

Table 1-2. Browser Interface Tools

Menu	Description
Configuration	This tool allows you to configure the system.
Monitoring	This tool allows you to view the status of the components and clients in the system, the connections on the local WFS709TP, WLANs, and custom logs.
Diagnostics	This tool allows you to run ping and traceroute, store and view output files for technical support, and view AP configuration and statistics.
Maintenance	This tool allows you to upgrade the image file, load licenses, copy files to/from flash, configure and reboot APs, and configure the captive portal feature
Plan	This tool enables you to design the WLAN deployment for your environment and provides coverage maps and AP and AM placement locations.
Events	This tool allows you to view events in the system and create event reports.
Reports	This tool allows you to view reports on APs (including rogue and interfering APs) and clients and create custom reports.

Configuration Tool

The Configuration pages are divided into two main branches: Basic pages provide a way to configure common network tasks, while the Advanced pages allow you to configure other features of the system.

Table 1-3 describes the Basic Configuration pages in the browser interface.

Table 1-3. Configuration Pages (Basic)

Page	Description
WLAN	These pages allow you to configure an SSID and related WLAN options.
Security	These pages allow you to configure the security Profile for Rogue AP detection.
Network	These pages allow you to configure ports, VLANs, IP interfaces, and DHCP-related information.
Management	These pages allow you to configure the system clock, SNMP-related information, and management access.
Access Point Installation Wizard	This page allows you to discover and configure Light Access Points connected to the Switch.

The following buttons are available on both the Basic and Advanced Configuration pages:

- **Apply.** Accepts all configuration changes made on the current page.
- **Save Configuration** (appears in top right corner of the browser interface when the Configuration tool is selected). Saves all applied configuration changes made during the current configuration session. Saved settings are retained when the WFS709TP is rebooted or powered off while unsaved configuration changes are lost.
- **Clear**. Resets options on current page to the last-applied or saved settings.
- **Add.** Adds a new item to the current page. Typically a set of relevant configuration fields for the item to be added is displayed.
- **Edit**. Allows you to edit the configuration of the selected item.
- **Delete**. Removes the selected item from the page configuration.

Note: By default, clicking Apply does *not* save the configuration. Once you finish configuring the switch, always remember to click Save Configuration.

Chapter 2
Deploying a Basic WFS709TP System

This chapter describes how to connect a WFS709TP ProSafe Smart Wireless Switch and access points (APs) to your wired network.

It includes the following topics:

Configuration Overview

This section describes the tasks you need to perform in connecting a WFS709TP and APs to your wired network in three typical deployment scenarios.

Deployment Scenario #1

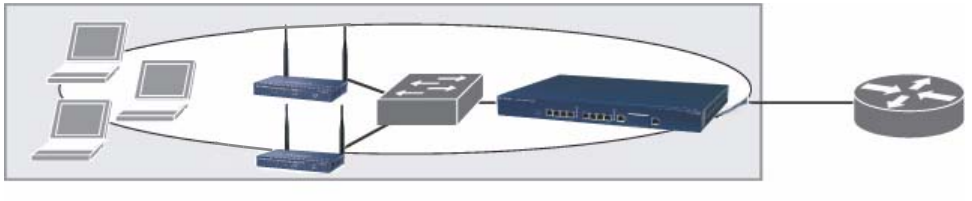

Figure 2-1

In the deployment scenario shown in Figure 2-1, the APs and WFS709TP are on the same subnetwork and will use IP addresses assigned to the subnetwork. There are no routers between the APs and the WFS709TP; APs can be physically connected directly to the WFS709TP. The uplink port on the WFS709TP is connected to a Layer 2 switch or router.

You need to perform the following tasks:

1. Run the initial setup (see"Run the Initial Setup" on page 2-6).

- Set the IP address of VLAN 1.
- Set the default gateway to the IP address of the interface of the upstream router to which you will connect the WFS709TP.

2. Connect the uplink port on the WFS709TP to the switch or router interface. By default, all ports on the WFS709TP are access ports and will carry traffic for a single VLAN.
3. Deploy the APs. The APs will use the ADP protocol to locate the WFS709TP.

You would then configure the SSIDs with VLAN 1 as the assigned VLAN for all users.

Deployment Scenario #2

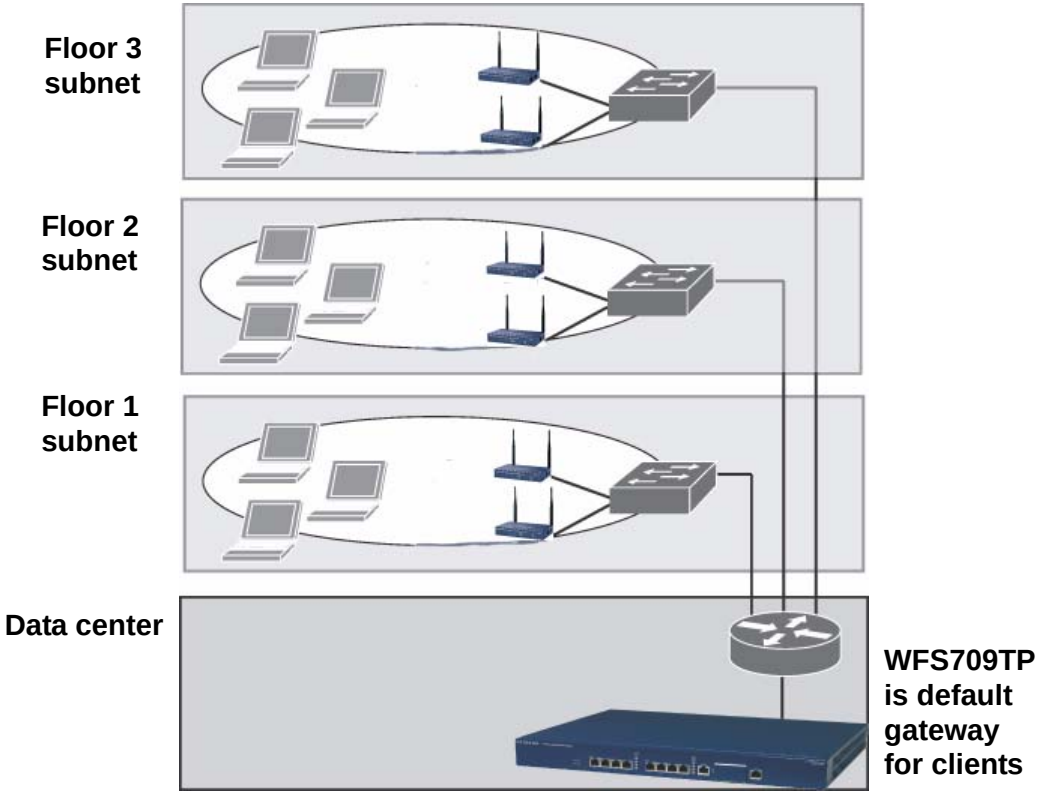

Figure 2-2

Figure 2-2 shows a deployment scenario where the APs and the WFS709TP are on different subnetworks and the APs are on multiple subnetworks. The WFS709TP acts as a router for the wireless user subnetworks. (It is the default gateway for the wireless clients.) The uplink port on the WFS709TP is connected to a Layer 2 switch or router; this port is an access port in VLAN 1.

You need to perform the following tasks:

1. Run the initial setup (see"Run the Initial Setup" on page 2-6).
   - Set the IP address for VLAN 1.
   - Set the default gateway to the IP address of the interface of the upstream router to which you will connect the WFS709TP.
2. Connect the uplink port on the WFS709TP to the switch or router interface.
3. Deploy the APs. The APs will use DNS or DHCP to locate the WFS709TP.

You would then need to configure VLANs for the wireless user subnetworks on the WFS709TP, and configure SSIDs with the VLANs assigned for each wireless user subnetwork.

Note: Each wireless user VLAN must be configured on the WFS709TP with an IP address. On the uplink switch or router, you must configure static routes for each user VLAN, with the WFS709TP's VLAN 1 IP address as the next hop.

Deployment Scenario #3

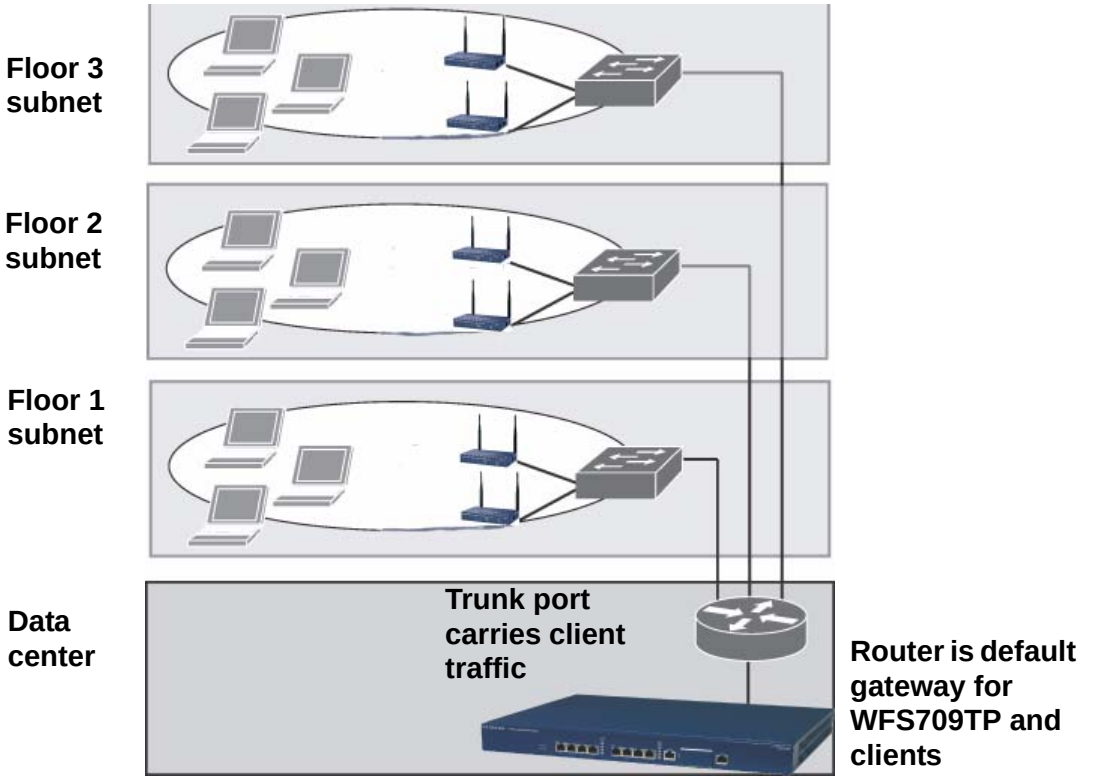

Figure 2-3

In this deployment scenario (Figure 2-3), the APs and the WFS709TP are on different subnetworks and the APs are on multiple subnetworks, with routers between the APs and the WFS709TP. The WFS709TP is connected to a Layer 2 switch or router through a trunk port that carries traffic for all wireless user VLANs. An upstream router functions as the default gateway for the wireless users.

	Note: This deployment scenario does *not* use VLAN 1 to connect to the Layer 2 switch or router through the trunk port. When the initial setup prompts you for the IP address and default gateway for VLAN 1, use the default values. In later steps, you will configure the appropriate VLAN to connect to the switch or router as well as the default gateway.

You need to perform the following tasks:

1. Run the initial setup (see"Run the Initial Setup" on page 2-6).
   - Use the *default* IP address for VLAN 1. Since VLAN 1 is not used to connect to the Layer 2 switch or router through the trunk port, you need to configure the appropriate VLAN in a later step.
   - Do *not* specify a default gateway (use the default "none"). In a later step, you configure the default gateway.
2. Create a VLAN that has the same VLAN ID as the VLAN on the switch or router to which you will connect the WFS709TP. Add the uplink port on the WFS709TP to this VLAN and configure the port as a trunk port.
3. Add user VLANs to the trunk port.
4. Configure the default gateway on the WFS709TP. This gateway is the IP address of the router to which you will connect the WFS709TP.
5. Configure the loopback interface for the WFS709TP.
6. Connect the uplink port on the WFS709TP to the switch or router interface.
7. Deploy the APs. The APs will use DNS or DHCP to locate WFS709TP.

You would then configure VLANs on the WFS709TP for the wireless user subnetworks and configure SSIDs with the VLANs assigned for each wireless user subnetwork.

Configuring the WFS709TP

The tasks in deploying a basic WFS709TP system fall into two main areas:

- Configuring and connecting the WFS709TP to the wired network (described in this section)
- Deploying APs (described later in this chapter)

To connect the WFS709TP to the wired network, you need to perform the following tasks:

1. Run the initial setup to configure administrative information for the WFS709TP.

2. ("Deployment Scenario #3" only) Configure a VLAN to connect the WFS709TP to your network.

> **Note:** You do not need to perform this step if you are using VLAN 1 to connect the WFS709TP to the wired network.

3. Connect the ports on the WFS709TP to your network.
4. (Optional) Configure a loopback address for the WFS709TP.

> **Note:** You do not need to perform this step if you are using the VLAN 1 IP address as the WFS709TP's IP address.

Run the Initial Setup

When you connect to theWFS709TP for the first time using either a serial console or a web browser, the initial setup automatically launches. The initial setup requires you to set a master or local role for the WFS709TP and passwords for administrator and configuration access. You must also specify the country code for the country in which the WFS709TP will operate; this sets the regulatory domain for the radio frequencies that the APs use.

The initial setup requires that you configure an IP address for the VLAN 1 interface, which you can use to access and configure the WFS709TP remotely via a Secure Shell (SSH) or browser interface session. Configuring an IP address for the VLAN 1 interface ensures that there is an IP address and default gateway assigned to the WFS709TP upon completion of the initial setup.

> **Warning:** Do not connect the WFS709TP Smart Wireless Switch to your network before you run the initial setup for these reasons:
>
> - The switch boots up with a default IP address which could interfere with your network.
> - The DHCP server on the switch is first enabled and then disabled after setup is complete. If you connect the switch to your network before completing the initial setup, the DHCP server is active on your network

To run the initial setup:

1. Connect the WFS709TP Smart Wireless Switch to your computer.
   a. Unpack the box and verify the contents.
   b. Prepare a PC with an Ethernet adapter.

      If this PC is already part of your network, record its TCP/IP configuration settings. Configure the PC with a static IP address of 192.168.0.200.
   c. Connect an Ethernet cable to the PC.
   d. Securely insert the other end of the cable into one of the Fast Ethernet Ports on the WFS709TP.
   e. Connect the power cord for the WFS709TP.
   f. Turn on your computer, open a web browser, and connect to http://192.168.0.250 (Figure 2-4).

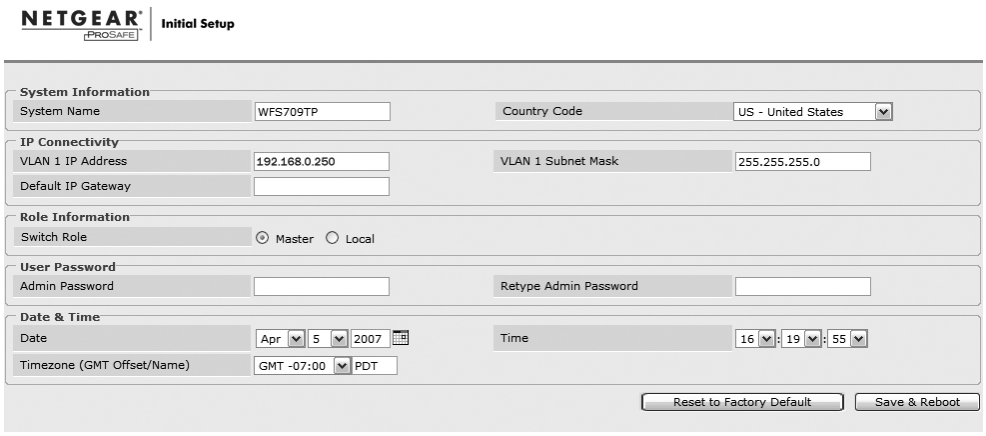

Figure 2-4

2. Enter the following information:
   - **System name**. A user-defined name for the switch (up to 64 characters).
   - **VLAN 1 IP address & subnetwork mask**—the IP address that the switch will use to communicate with other switches and with access points.
   - **Default gateway**. The default gateway on the switch's planned subnetwork (the default gateway and VLAN 1 IP address must be in the same network).
   - **Role**. Enter one of these roles for the switch:

  - Master (if this will be the only switch on the network)
  - Local (if this will be managed by a master switch)
- **Country code**. The two-letter code for the country in which the switch will operate from the drop-down menu.

  This determines the 802.11 wireless transmission spectrum. You are responsible for assigning the correct country code and for changing it if the switch is moved to another country. Improper country code assignment can disrupt wireless transmissions. Most countries impose penalties and sanctions for operators of wireless networks with devices set to improper country codes.
- **Master switch IP** (if the switch is local). The IP address of this switch's master switch.
- **Admin user password**. For logging into the switch (up to 32 characters).

  You must enter this password in order to further configure the switch; there is no factory provided password.
- **Date and time**. Time, date, and time zone. (If you are going to use an NTP server, the switch will pick up the date and time from this server later.)

3. Click Save and Reboot.

   The switch will reboot, using the new configuration. (This can take up to 2 minutes). After reboot you will probably not have network connectivity on your PC. Reconfigure your PC to match the settings you just configured for the switch and then proceed to the access point configuration.

	**Note:** Later, if needed, you can reconfigure the PC you used in step 1 back to its original TCP/IP settings.

Configure the Switch for the Access Points

1. Connect the WFS709TP Smart Wireless Switch to your PC using an Ethernet cable to one of the Fast Ethernet Ports.
2. In the web browser of your PC:
   a. Enter the IP address of your master switch. See step 2 of "Run the Initial Setup" on page 2-6.
   b. Log in using the admin user account and password (Figure 2-5). See step 2 of "Run the Initial Setup" on page 2-6.

Figure 2-5

c. In the Configuration UI, click the Configuration tab>Advanced option>DHCP Server, then enter the information to configure the DHCP server. (Figure 2-6)

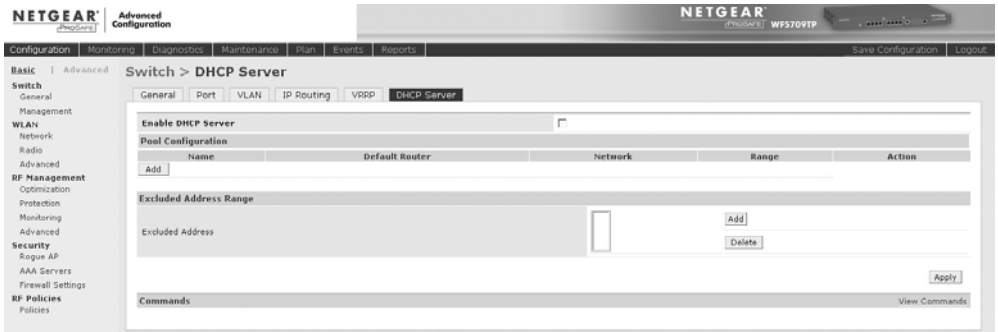

Figure 2-6

Connect the access points directly to the switch using an Ethernet cable to one of the Fast Ethernet Ports on the switch (this does not need to be the final installation location for the access points). Allow up to 10 minutes for the switch to locate and download firmware to the access point(s).

3. In the web browser of your PC, navigate to the Access Point Installation Wizard:

a. Verify that the access point(s) are detected by the system by clicking the Configuration tab > Basic option > Access Point Installation Wizard > Monitoring. Unconfigured access points will be listed as unprovisioned.

b. Follow the prompts of the Wizard to complete configuration of the switch for all access points.

4. Refer to the documentation included with the access points to complete their installation.

Configure a VLAN for Network Connection

Follow the instructions in this section only if you need to configure a trunk port between the WFS709TP and another Layer 2 switch (as in "Deployment Scenario #3" on page 2-4).

This section shows how to use the browser interface for the following configurations:

- Create a VLAN on the WFS709TP and assign it an IP address.
- Assign to the VLAN the port or ports that you will use to connect the WFS709TP to the network. (For example, the uplink ports that you connect to a router are usually Gigabit ports.)
- Configure the ports as trunk ports.
- Configure a default gateway for the WFS709TP.

Note: In the browser interface configuration pages, clicking the Apply button saves configuration changes so they are retained after the WFS709TP is rebooted.

Create the VLAN

The following configurations create VLAN 5 and assign it the IP address 10.3.22.20/24.

1. Navigate to the Configuration > Basic > Network >VLAN page.
2. Click Add to create a new VLAN.
3. On the Add New VLAN screen (Figure 2-7), enter 5 for the VLAN ID and click Apply.

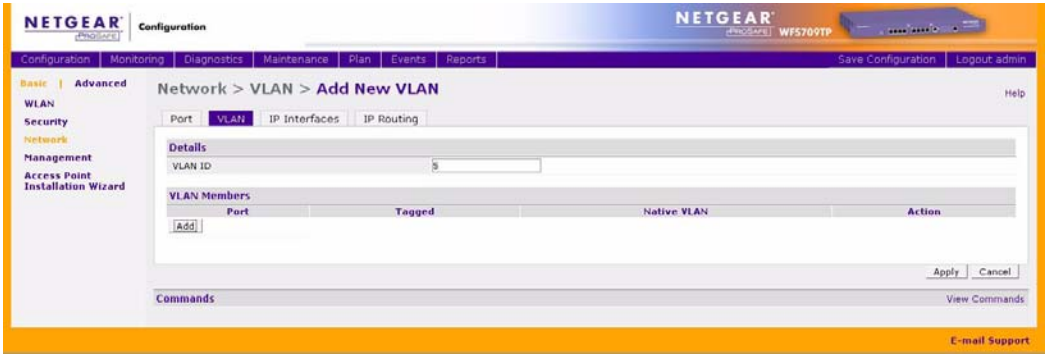

Figure 2-7

4. Navigate to the Configuration > Basic > Network > IP Interfaces page (Figure 2-8). Click Edit for the VLAN you just added. Enter the IP address and network mask of the VLAN interface. If required, you can also configure the address of the DHCP server for the VLAN by clicking Add.

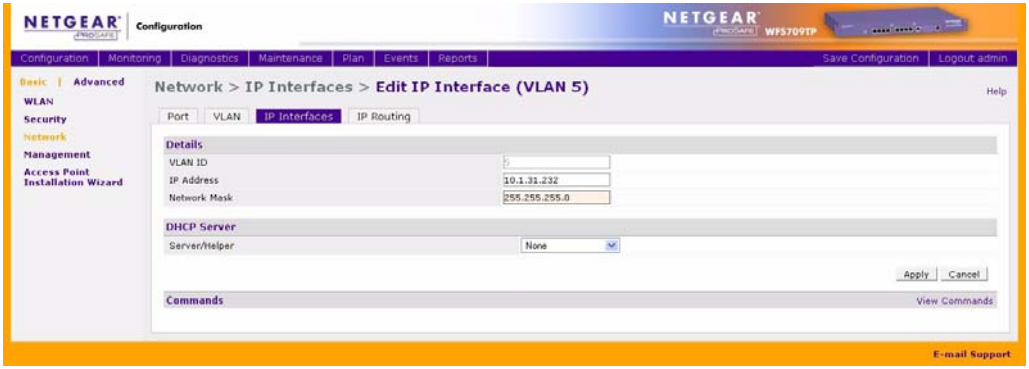

Figure 2-8

5. Click Apply to apply and save this configuration.

Configure the Trunk Port

The following procedure configures a Gigabit Ethernet port as a trunk port.

1. Navigate to the Configuration > Basic > Network > Port page (Figure 2-8).
2. To add a port to the VLAN, click the port in the Port Selection section.
3. For Port Mode, select Trunk.
4. For Native VLAN, select VLAN 5 from the scrolling list, then click the ← arrow.

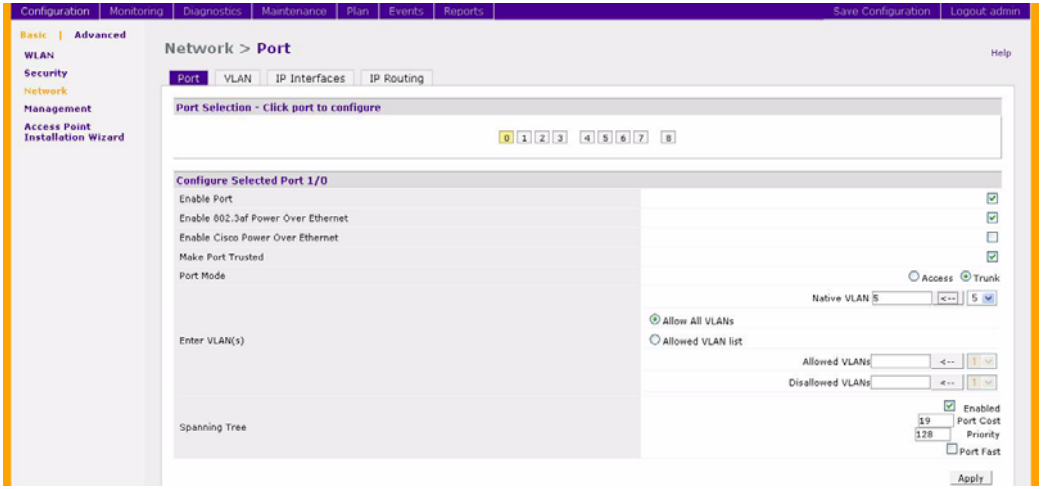

Figure 2-9

5. Click Apply.

Configure the Default Gateway

The following configuration assigns a default gateway for the WFS709TP.

1. Navigate to the Configuration > Advanced > Switch > General > IP Routing page.
2. In the Default Gateway field, enter 10.3.22.1.
3. Click Apply.

Connect the WFS709TP to the Network

Connect the ports on the WFS709TP to the appropriately configured ports on an L2 switch or router. Make sure that you have the correct cables and that the port LEDs indicate proper connections. Refer to the document *WFS709TP ProSafe Smart Wireless Switch Hardware Installation Guide* for port LED and cable descriptions.

Note: You can find the *WFS709TP ProSafe Smart Wireless Switch Hardware Installation Guide* in PDF form on the WFS709TP *Resource CD*. It is also available from the NETGEAR support site at *http://www.netgear.com/support*.

To verify that the WFS709TP is accessible on the network:

- If you are using VLAN 1 to connect the WFS709TP to the network (see "Deployment Scenario #1" on page 2-1 and "Deployment Scenario #2" on page 2-2), ping the VLAN 1 IP address from a workstation on the network.
- If you created and configured a new VLAN (see "Deployment Scenario #3" on page 2-4), ping the IP address of the new VLAN from a workstation on the network.

Configure the Loopback for the WFS709TP

You need to configure a loopback address if you are not using VLAN 1 to connect the WFS709TP to the network ("Deployment Scenario #3"). The loopback address is used as the WFS709TP's IP address. If you do not configure a loopback address, the IP address assigned to VLAN 1 is used as the WFS709TP's IP address.

Note: After you configure or modify a loopback address, you must reboot the WFS709TP for the change to take effect.

The loopback address can be part of the IP address space assigned to a VLAN interface. In the example topology used in the procedure "Create the VLAN" on page 2-10, the VLAN 5 interface on the WFS709TP was previously configured with the IP address 10.3.22.20/24. The loopback IP address in this example will be 10.3.22.220.

Note: You configure the loopback address as a host address with a 32-bit netmask. The loopback address should be routable from all external networks.

To set the loopback address through the browser interface:

1. Navigate to the Configuration > Advanced > Switch > General page (Figure 2-10).
2. Enter the IP address for the loopback address.

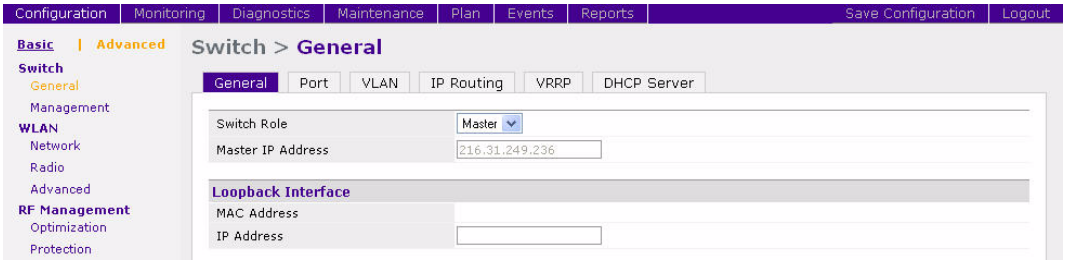

Figure 2-10

3. Click Apply at the bottom of the page (you may need to scroll down the page).
4. At the top of the page, click Save Configuration.

   You need to reboot the WFS709TP for the new IP address to take effect.
5. Navigate to the Maintenance > Switch > Reboot Switch page (Figure 2-11).

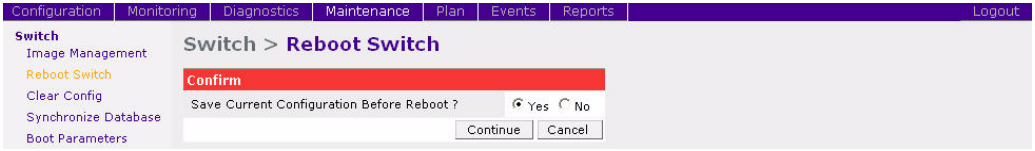

Figure 2-11

6. Click Continue.

Deploying APs

APs and AMs are designed to require only minimal provisioning to make them fully operational in a WFS709TP system. Once APs have established communication with the WFS709TP, you can apply advanced configuration to individual APs or globally across the entire system using the browser interface on the WFS709TP.

You can deploy APs from the browser interface by performing the following tasks:

1. Ensure that the APs can locate the WFS709TP when they are connected to the network. There are several ways in which APs can locate the WFS709TP (see “Locate the WFS709TP” on page 2-16).
2. Install the APs by connecting the AP to an Ethernet port and, optionally, to a power source.

3. On the WFS709TP, configure the APs. (See “Configure the Switch for the Access Points” on page 2-8)

The following sections describe the steps for these tasks.

Enable APs to Connect to the WFS709TP

Before you install APs in a network environment, you must ensure that the APs will be able to connect to the WFS709TP when powered on. Specifically, you need to ensure the following:

- When connected to the network, each AP is assigned a valid IP address
- The APs are able to locate the WFS709TP

	**Note:** All APs designed or modified to work with the WFS709TP use Trivial File Transfer Protocol (TFTP) the first time they boot to obtain their software image and configuration from the WFS709TP. After their initial boot, the APs use FTP to obtain software images and configurations from the WFS709TP.

Enable APs to Obtain IP Addresses

Each AP requires a unique IP address on a subnetwork that has connectivity to a WFS709TP. NETGEAR recommends using the Dynamic Host Configuration Protocol (DHCP) to provide IP addresses for APs. The DHCP server can be an existing network server or a WFS709TP configured as a DHCP server.

You can use an existing DHCP server in the same subnetwork as the AP to provide the AP with its IP information. You can also configure a device in the same subnetwork to act as a relay agent for a DHCP server on a different subnetwork. Refer to the vendor documentation for your DHCP server or relay agent for more information.

If an AP is on the same subnetwork as the master WFS709TP, you can configure the WFS709TP as a DHCP server to assign an IP address to the AP. The WFS709TP must be the only DHCP server for this subnetwork.

To enable DHCP server capability on a WFS709TP:

1. Navigate to the Configuration > Advanced > Switch > General > DHCP Server page (Figure 2-12).

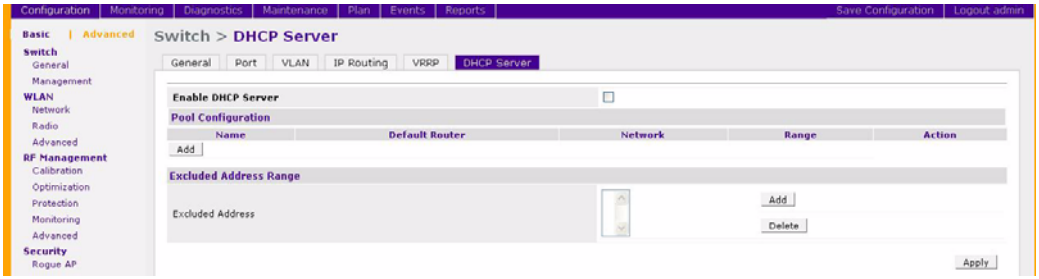

Figure 2-12

2. Select the Enable DHCP Server checkbox.
3. In the Pool Configuration section, click Add.

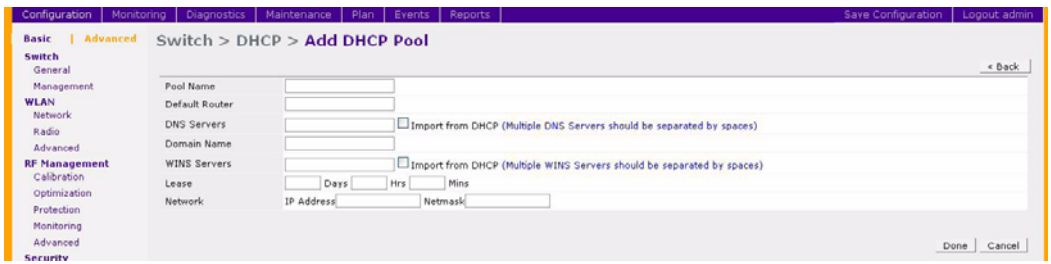

Figure 2-13

4. On the Add DHCP Pool page, enter information about the subnetwork for which IP addresses are to be assigned (Figure 2-13). Click Done.
5. If there are addresses that should not be assigned in the subnetwork:
   a. Click Add in the Excluded Address Range section.
   b. Enter the address range in the Add Excluded Address section.
   c. Click Done.
6. Click Apply at the bottom of the page.
7. At the top of the page, click Save Configuration.

Locate the WFS709TP

An AP can discover the IP address of the WFS709TP in one of the following ways:

- From a DNS server

- From a DHCP server
- Using the ADPprotocol

From a DNS Server. NETGEAR APs are factory-configured to use the host name **netgear-master** for the WFS709TP. For the DNS server to resolve this host name to the IP address of the WFS709TP you must configure an entry on the DNS server for the name **netgear-master**.

Using a DNS server to provide APs with the IP address of the master WFS709TP involves minimal changes to the network and provides the greatest flexibility in the placement of APs.

Note: For information on how to configure a host name entry on the DNS server, refer to the vendor documentation for your server.

From a DHCP Server. You can configure a DHCP server to provide the WFS709TP's IP address. You need to configure the DHCP server to send the WFS709TP's IP address using the DHCP vendor-specific attribute option 43. NETGEAR APs identify themselves with a vendor class identifier set to **NetgearAP** in their DHCP request. When the DHCP server responds to the request, it will send the WFS709TP's IP address as the value of option 43.

Note: For more information on how to configure vendor-specific information on a DHCP server, see Appendix A, "Configuring DHCP with Vendor-Specific Options" or refer to the vendor documentation for your server.

Using ADP. The Aruba Discovery Protocol (ADP) is enabled by default on all NETGEAR APs and WFS709TPs. To use ADP, all APs and WFS709TPs must be connected to the same Layer 2 network. If the devices are on different networks, a Layer 3-compatible discovery mechanism, such as DNS, DHCP, or Internet Group Management Protocol (IGMP) forwarding, must be used instead.

With ADP, APs send out periodic multicast and broadcast queries to locate the WFS709TP. You may need to perform additional network configuration, depending on whether the APs are in the same broadcast domain as the WFS709TP:

- If the APs are in the same broadcast domain as the WFS709TP, the WFS709TP automatically responds to AP queries with its IP address.

- If the APs are not in the same broadcast domain as the WFS709TP, you need to enable multicast on the network for the WFS709TP to respond to the AP queries. ADP multicast queries are sent to the IP multicast group address 224.0.82.11. You also need to make sure that all routers are configured to listen for IGMP join requests from the WFS709TP and that they can route these multicast packets.

Install APs

When deploying APs, note the AP's MAC address and serial number as well as its physical location on the placement map. This is useful in assigning location code identifiers to APs (see "To configure the location code for an AP:" on page 2-18), which greatly enhances location-based services and wireless network calibration.

You can either connect the AP directly to a port on the WFS709TP, or connect the AP to another switch or router that has Layer 2 or Layer 3 connectivity to the WFS709TP.

If the Ethernet port is an 802.3af Power over Ethernet (PoE) port, the AP automatically uses it to power up. If a PoE port is not available, use the AC adapter shipped with the access point to power the AP.

Once an AP is connected to the network and powered up, it attempts to locate its WFS709TP using one of the methods described in "Locate the WFS709TP" on page 2-16.

Provision APs

The next step in AP deployment is to configure or provision each AP. You must minimally configure each AP with a unique location code that is used for location servicing. The location code is in the numerical format *1.2.3*, where *1* specifies the building, 2 specifies the floor, and *3* specifies the location.

You can also configure IntelliFi RF Management (IRM), a mechanism that enables NETGEAR APs to optimize their functions in any RF environment. (See "Automatic RF Channel and Power Settings" on page 1-4.)

To configure the location code for an AP:

1. Navigate to the Maintenance > Program AP page (Figure 2-14).

This page displays a list of APs that have registered with the WFS709TP with either their default location code (-1.-1.-1) or their currently configured location code (if the AP has already been provisioned).

Figure 2-14

2. Select the AP that is to be configured from the list by selecting the checkbox to the left of the AP and then clicking the Provision button.

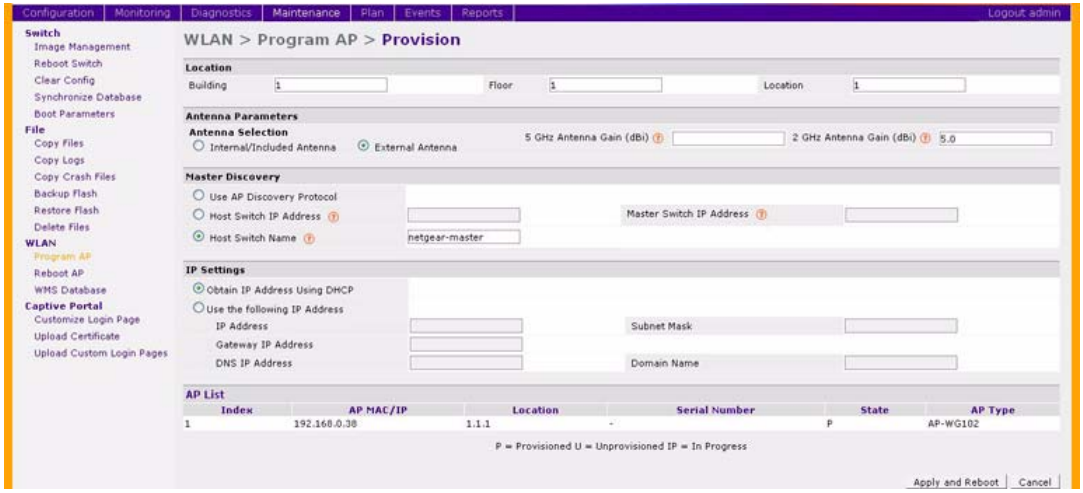

Figure 2-15

3. On the Provision page (Figure 2-15), enter the location code in the format explained at the beginning of this section.

4. Enter the antenna gain in dBi (for example, enter 5.0). This information is mandatory, as the AP cannot bring up its radio interface or function as an AP without it.

5. Click Apply and Reboot to apply the configuration to the AP.

	Note: The configuration does not take effect until the AP is rebooted

Additional Configuration

After you have installed a basic WFS709TP system, the APs advertise the default **netgear-ap** SSID. Wireless users can connect to this SSID, but because you have not yet configured authentication, policies, or user roles, they will not have access to the network. Other chapters in this manual describe how to build upon this basic deployment to configure user roles, authentication, authentication servers, and other wireless features.

Chapter 5, “Configuring WLANS” describes how to configure WLANs using the browser interface. If you used the AP Installation Wizard in the browser interface to program and install your APs, you are redirected to the WLAN Basic Configuration page where you can configure the SSID and authentication for a WLAN.

Chapter 3
Configuring Network Parameters

This chapter describes basic network configuration on the WFS709TP ProSafe Smart Wireless Switch. It includes the following topics:

Configuring VLANs

The WFS709TP ProSafe Smart Wireless Switch operates as a Layer 2 switch that uses a VLAN as a broadcast domain. As a Layer 2 switch, the WFS709TP requires an external router to route traffic between VLANs. The WFS709TP can also operate as a Layer 3 switch that can route traffic between VLANs defined on the switch.

You can configure one or more physical ports on the WFS709TP to be members of a VLAN. Additionally, each wireless client association constitutes a connection to a virtual port on the switch, with membership in a specified VLAN. You can place all authenticated wireless users into a single VLAN or into different VLANs, depending upon your network. VLANs can exist only inside the WFS709TP; you must use 802.1q VLAN tagging to extend them outside the switch.

You can optionally configure an IP address and netmask for a VLAN on the WFS709TP. The IP address is up when at least one physical port in the VLAN is up. The VLAN IP address can be used as a gateway by external devices; packets directed to a VLAN IP address that are not destined for the switch are forwarded according to the WFS709TP's IP routing table.

Creating a VLAN

To create or edit a VLAN:

1. Navigate to the Configuration > Basic > Network > VLAN page on the browser interface.
2. Click Add to create a new VLAN. (To edit an existing VLAN, click Edit for the VLAN entry.)

3. On the Add New VLAN screen (Figure 3-1), enter the VLAN ID.

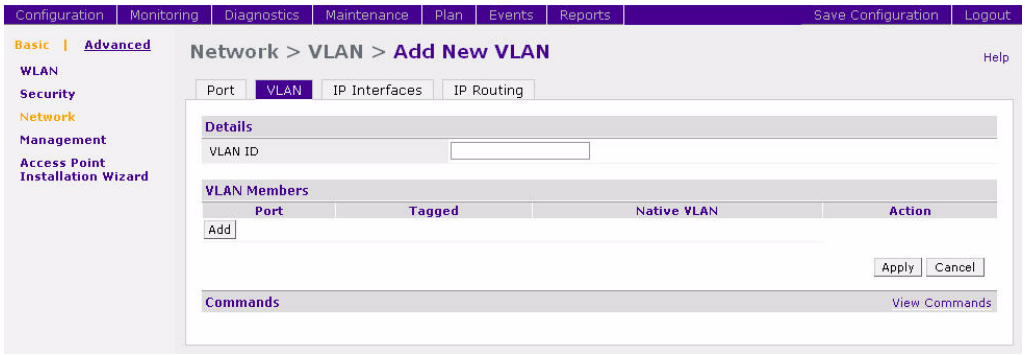

Figure 3-1

4. To add physical ports to the VLAN, click Add in the VLAN Members section, then select the port to add to the VLAN.
   - You can specify whether the port uses 802.1q tagging.
   - For ports that use 802.1q tagging, you can also specify whether the VLAN is the native VLAN for the port (frames on the native VLAN are not tagged).
5. Click Add.
6. Click Apply.

Assigning a Static Address to a VLAN

To assign a static IP address to a VLAN:

1. Navigate to the Configuration > Basic > Network > IP Interfaces page on the browser interface (Figure 3-2).
2. Click Edit for the VLAN you just added.

3. Enter the IP address and network mask of the VLAN interface. If required, you can also configure the address of the DHCP server for the VLAN by clicking Add.

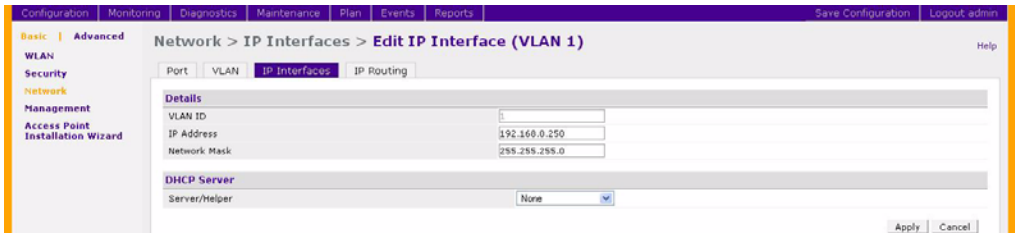

Figure 3-2

4. Click Apply.

Configuring a VLAN to Receive a Dynamic Address

A VLAN on the WFS709TP obtains its IP address in one of the following ways:

- Manually configured by the network administrator. This is the default method and is described in "Assigning a Static Address to a VLAN" on page 3-2. At least one VLAN on the switch must be assigned a static IP address.
- Dynamically assigned from a Dynamic Host Configuration Protocol (DHCP) server. These methods are described in the following section.

In a branch office, you can connect a WFS709TP to an uplink switch or server that dynamically assigns IP addresses to connected devices. For example, the switch can be connected to a DSL or cable modem, or a broadband remote access server (BRAS). Figure 3-3 shows a branch office where a WFS709TP connects to a cable modem. VLAN 1 has a static IP address, while VLAN 2 has a dynamic IP address assigned via DHCP on the uplink device. The DHCP server on the WFS709TP assigns IP addresses to users on the local network from a configured pool of IP addresses.

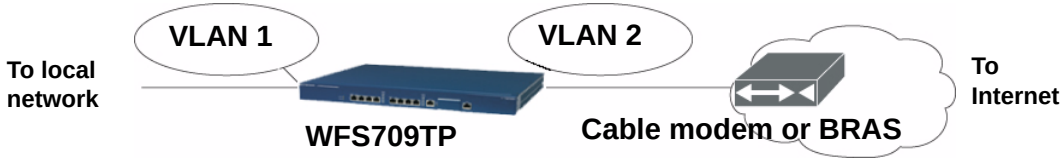

Figure 3-3

To allow the WFS709TP to obtain a dynamic IP address for a VLAN, you enable the DHCP client on the WFS709TP for the VLAN.

The following restrictions apply when enabling DHCP on the WFS709TP:

- You can enable the DHCP client on only one VLAN on the WFS709TP; this VLAN cannot be VLAN 1.
- Only one port in the VLAN can be connected to the modem or uplink switch.
- At least one interface in the VLAN must be in the up state before the DHCP client requests an IP address from the server.
- Only one VLAN on the WFS709TP can obtain its IP address through DHCP.

Enabling the DHCP Client

The DHCP server assigns an IP address for a specified amount of time called a *lease*. The switch automatically renews the lease before it expires. When you shut down the VLAN, the DHCP lease is released.

To enable the DHCP client on a VLAN:

1. Navigate to the Configuration > Advanced > Switch > General > VLAN page.
2. Click Add to create a new VLAN or click Edit for a previously created VLAN.
3. Select Obtain an IP address from DHCP.
4. Select the port that is connected to the modem or uplink switch.
5. Click Apply.

Default Gateway from DHCP

You can specify that the router IP address obtained from the DHCP server be used as the default gateway for the switch. To do this:

1. Navigate to the Configuration > Advanced > Switch > IP Routing page.
2. For Default Gateway, select Obtain an IP address automatically.
3. Select Apply.

DNS/WINS Server from DHCP

The DHCP server can also provide the IP address of a Domain Name Service (DNS) server or NetBIOS name server, which can be passed to wireless clients through the switch’s internal DHCP server.

For example, the following steps configure the DHCP server on the WFS709TP to assign addresses to authenticated employees; the IP address of the DNS server obtained by the WFS709TP via DHCP is provided to clients along with their IP address.

1. Navigate to the Configuration > Advanced > Switch > General > DHCP Server page.
2. Select Enable DCHP Server.
3. Under Pool Configuration, select Add.
4. For Pool Name, enter **employee-pool**.
5. For Default Router, enter 10.1.1.254.
6. For DNS Servers, select Import from DHCP.
7. For WINS Servers, select Import from DHCP.
8. For Network, enter 10.1.1.0 for IP Address and 255.255.255.0 for netmask.
9. Click Done.

Configuring Static Routes

To configure a static route (such as a default route) on the WFS709TP, do the following:

1. Navigate to the Configuration > Advanced > Switch > General > IP Routing page (Figure 3-4).
2. Click Add to add a static route to a destination network or host. Enter the destination IP and network mask (255.255.255.255 for a host route) and the next-hop IP address.

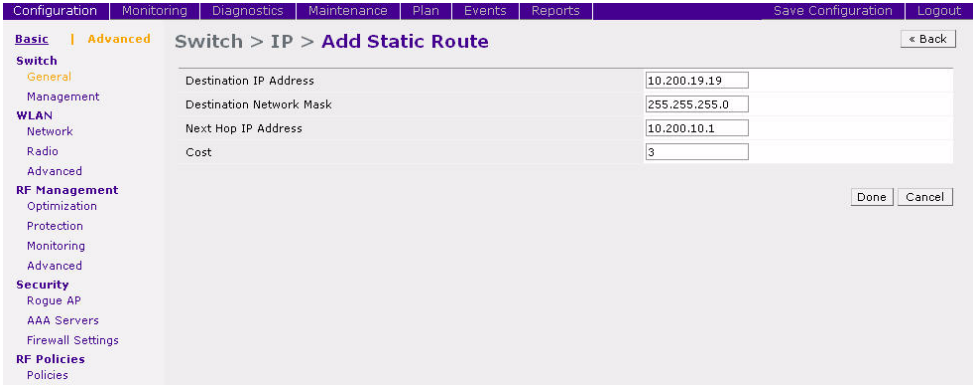

Figure 3-4

3. Click Done to add the entry.

	**Note:** The route has not yet been added to the routing table.

4. Click Apply to add this route to the routing table.

   The message Configuration Updated Successfully confirms that the route has been added.

Configuring the Loopback IP Address

The loopback IP address is a logical IP interface that is used by the WFS709TP to communicate with APs. If you do not configure a loopback address for the switch, the IP address of the lowest-numbered VLAN interface (typically VLAN 1) is used.

The WFS709TP uses the loopback address as its IP address for terminating Virtual Private Network (VPN) and Generic Routing Encapsulation (GRE) tunnels, for originating requests to RADIUS servers, and for accepting administrative communications. You configure the loopback address as a host address with a 32-bit netmask. The loopback address is not bound to any specific interface and is operational at all times. To make use of this interface, ensure that the IP address is reachable through one of the VLAN interfaces. It should be routable from all external networks.

You can modify or delete the IP address of the loopback interface on the WFS709TP. However, you cannot delete the loopback address if there is no IP address configured for the VLAN 1 interface; if you attempt to do so, you will be prompted for a new IP address for the VLAN 1 interface. You also cannot delete the IP address for the VLAN 1 interface if there is no loopback address configured; you will be prompted for a new loopback address.

	**Note:** Any change in the WFS709TP's IP address requires a reboot.

To configure or change the loopback IP address on the WFS709TP:

1. Navigate to the Configuration > Advanced > Switch > General page on the browser interface (Figure 3-5).

Figure 3-5

2. Modify the loopback IP address in the Loopback Interface section on this page as required. Click Apply to apply this configuration.

	**Warning:** If you are using the loopback IP address to access the browser interface, changing the loopback IP address will result in loss of connectivity. Use one of the VLAN interface IP addresses to access the browser interface.

3. Navigate to the Maintenance > Switch > Reboot Switch page (Figure 3-6) to reboot the WFS709TP and apply the change of loopback IP address.

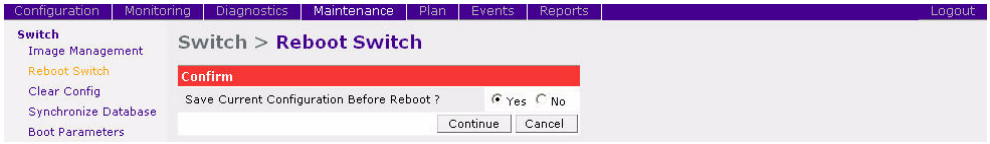

Figure 3-6

4. Click Continue to save the configuration.
5. When prompted that the changes were written successfully to flash (Figure 3-7), click OK.

Figure 3-7

The WFS709TP boots up with the changed loopback IP address.

Chapter 4
RF Plan

RF Plan is a built-in wireless deployment modeling tool that enables you to design an efficient wireless local area network (WLAN) for your corporate environment, optimizing coverage and performance, and eliminating complicated WLAN network setup.

This chapter describes the following topics:

RF Plan Overview

RF Plan provides the following functionality:

- Defines WLAN coverage
- Defines WLAN environment security coverage
- Assesses equipment requirements
- Optimizes radio resources

RF Plan provides a view of each floor, allowing you to specify how Wi-Fi coverage should be provided. It then provides coverage maps and access point (AP) and air monitor (AM) placement locations. Real-time calibration lets you characterize the indoor propagation of RF signals to determine the best channel and transmission power settings for each AP or AM. You can program the calibration to occur automatically, or you can manually launch the calibration at any time to quickly adapt to changes in the wireless environment.

Before You Begin

Before you use RF Plan, review the following steps to create a building model and plan the WLAN for the model.

Task Overview

1. Gather information about your building's dimensions and floor plan.
2. Determine the level of coverage you want for your APs and AMs.
3. Create a new building and add its dimensions.
4. Enter the parameters of your AP coverage.
5. Enter the parameters of your AM coverage.
6. Add floors to your building and import the floor plans.
7. Define special areas.
8. Generate suggested AP and AM tables by executing the AP/AM Plan features.

Planning Requirements

Collect the following information before using RF Plan to expedite your planning efforts.

- Building dimensions
- Number of floors
- Distance between floors
- Number of users and number of users per AP
- Radio type or types
- Overlap factor
- Desired data rates for APs
- Desired monitoring rates for AMs
- Areas where you do not necessarily want coverage
- Areas where you do not want or cannot deploy an AP or AM
- Any area where you want to deploy a fixed AP or AM

Use a worksheet similar to the following to collect your information:

Table 4-1.

Building Dimensions	
Height:	Width:
Number of Floors:	
User Information	
Number of Users:	Users per AP:
Radio Types:	
Overlap Factor:	
AP Desired Rates	
802.11b|g:	802.11a:
AM Desired Rates	
802.11b|g:	802.11a:
Don't Care/Don't Deploy Areas:	

Using RF Plan

This section describes how to use RF Plan and how to enter information in RF Plan pages.

To start RF Plan, click the Plan tab in the browser interface menu bar.

When you start RF Plan, the browser window shows the Building List page (Figure 4-1).

Figure 4-1

Building List Page

Building List is the first page you see when you start RF Plan. This list contains all the buildings you have defined using the RF Plan tool. The first time you run the application, there are no buildings in the list.

You can add, edit, and delete buildings using this page. You can also import and export building information. This page includes the following buttons:

- **New Building**. Use this button to create a new building.
- **Edit Buildings**. Use this button to edit existing buildings in the building list. To edit a building, select the checkbox next to the building ID, then click Edit Building.

> **Note:** When you add or edit a building, you can access other RF Plan pages

- **Delete Buildings**. Use this button to delete existing buildings in the building list. To delete a building, select the checkbox next to the building ID, then click Delete Building.
- **Export.** Use this button to export a database file with all the specifications and background images of one or more selected buildings in the building list.
- **Import**. Use this button to import database files that define buildings into the RF Plan building list.

> **Note:** See "Exporting and Importing Files" on page 4-20 for more information about exporting and importing RF Plan database files.

- **Locate**. Use this button to find a building.

Building Specification Overview Page

The Building Specification Overview page (Figure 4-2) shows the default values for a building that you are adding or the current values for a building that you are modifying.

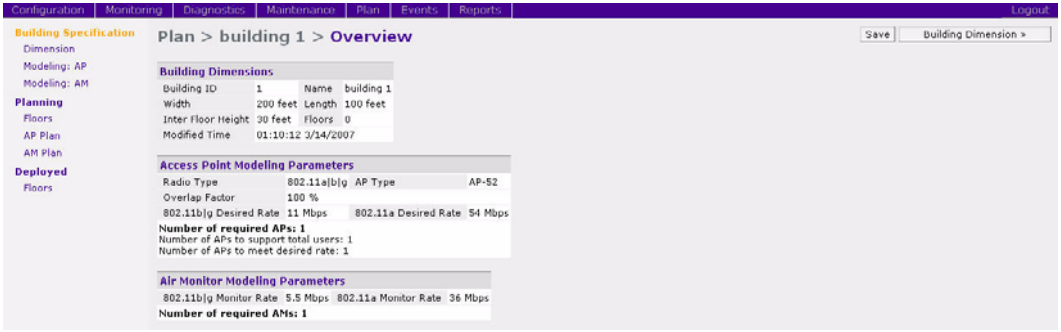

Figure 4-2

The Overview page includes the following:

- **Building Dimensions**. Your building's name and dimensions
- **Access Point Modeling Parameters**.
- **Air Monitor Modeling Parameters**.
- **Building Dimensions button** (in the upper right of the page). Click this button to edit the building dimensions settings.

There are several ways you can navigate through RF Plan pages when you create or edit information for a building.

- The navigation pane on the left side of the browser window displays RF Plan pages in the order in which they should be accessed when you are creating a new building. If you are editing a building, simply click the name of the page you want to display or modify.
- A button for the next page appears in the upper right of the page. You can click this button to display the next page in the sequence. For example, the Building Dimension button appears in the Building Specification Overview page.
- Clicking Apply on editable pages also sequences you to the next page. For example, when you click Apply in the Building Dimension page, the AP Modeling Parameters page displays.

Building Dimension Page

The Building Dimension page (Figure 4-3) allows you to specify the name and identification for the building and its dimensions.

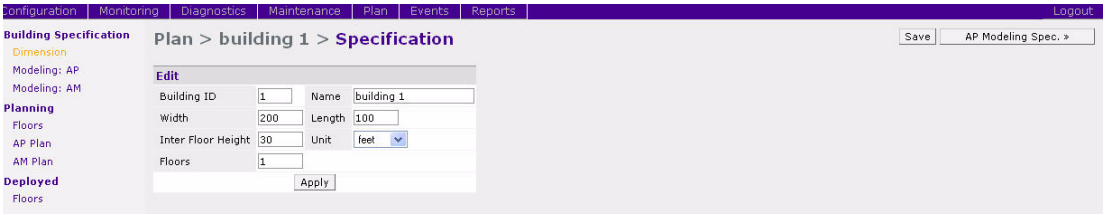

Figure 4-3

Enter the following information:

- **Building ID.** The valid range for this field is any integer from 1 to 255.
- **Building Name**. The Building Name is an alphanumeric string up to 64 characters in length.
- **Width and Length**. Enter the rectangular exterior dimensions of the building. The valid range for this field is any integer from 1 to a value corresponding to $1x10^{12}$.

  If your building has an irregular shape, the width and length should represent the maximum width and length of the overall footprint of the building as seen from above. Figure 4-4 shows how to measure the coverage area for irregular shapes.

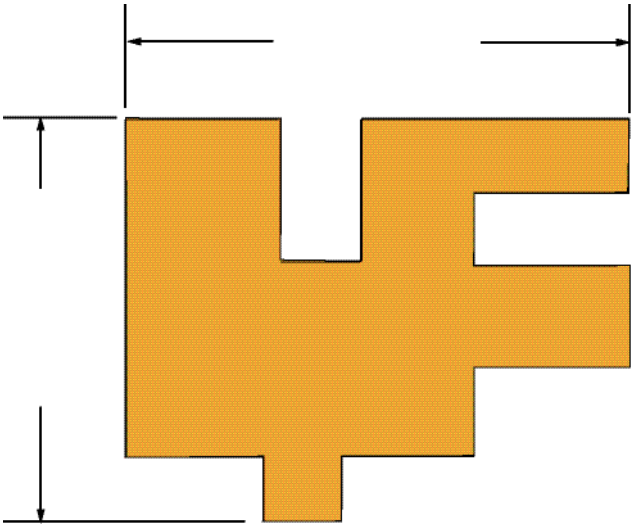

Figure 4-4

When width and length are specified, RF Plan creates a rectangular area in the Planning feature pages that represent the overall area covered by the building. You need to import an appropriate background image ("Floor Editor Dialog Box" on page 4-12) to aid you in defining areas that don't require coverage or areas in which you do not wish to deploy APs and AMs ("Area Editor Dialog Box" on page 4-13).

- **Inter-Floor Height.** This is the distance between floor surfaces in the building.

> **Note:** The inter-floor height is *not* the distance from floor to ceiling. Some buildings have a large space between the interior ceilings and the floor above.

The valid range for this field is any integer from 1 to a value corresponding to $1x10^{12}$.

- **Floors.** Enter the number of floors in your building. The valid range for this field is any integer from 1 to a value corresponding to $1x10^{12}$.
- **Unit**. Specify the unit of measurement for the dimensions you specified on the page. The choices are feet and meters.

AP Modeling Parameters Page

The AP Modeling Parameters page (Figure 4-5) allows you to specify the information necessary for RF Plan to determine the appropriate placement of your APs.

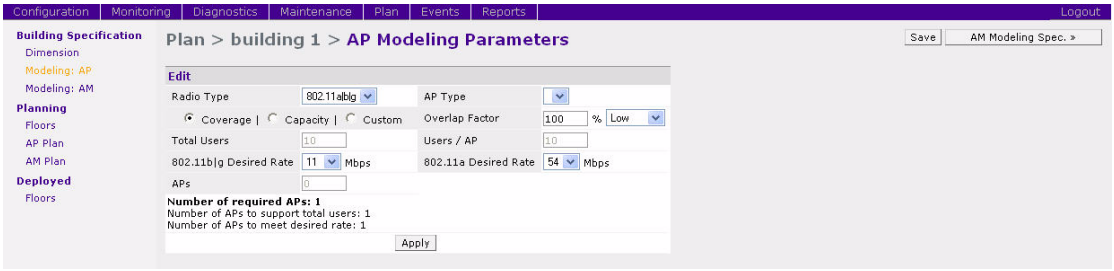

Figure 4-5

Controls on this page allow you to select or control the following functions, which are described in further detail in this section:

- **Radio Type.** Use this pull-down menu to specify the radio type.
- **AP Type.** Use this drop-down box to select the AP model.
- **Overlap Factor.** Use this field and pull-down to specify an AP coverage overlap factor.

- **Design Model.** Use these radio buttons to specify which design model to use in the placement of APs.
- **Users.** Use this field to specify the number of users on your WLAN.
- **Rates**. Use this pull-down to specify the data rates desired on APs.

Radio Type

Specify the radio type or types of your APs using the pull-down Radio Type menu. Available Radio Type choices are:

- **801.11a.** 5-GHz, Orthogonal Frequency Division Multiplexing (OFDM) with data rates up to 54 Mbps.
- **802.11b.** 2.4-GHz, Direct Spread Spectrum (DSSS) multiplexing with data rates up to 11 Mbps.
- **802.11g.** 2.4-GHZ, OFDM/CCK (Complementary Code Keying) with data rates up to 54 Mbps.

Overlap Factor

The overlap factor is the amount of signal area overlap when the APs are operating. Overlap is important if an AP fails, as it allows the network to self-heal with adjacent APs powering up to assume some of the load from the failed device. Although there might be no holes in coverage in when this occurs, there is likely to be a loss of throughput. Increasing the overlap allows for higher throughputs when an AP has failed, and also allows for future capacity as the number of users increases.

The valid range of values for the overlap factor is from 100% to 1000%.

Design Model

Three radio buttons on the page allow you to control the kind of model used to determine the number and type of APs:

- **Coverage.** Use this option to let RF Plan automatically determine the number of APs based on desired data rates and the configuration of your building.
- **Capacity.** Use this option to let RF Plan determine the number of APs based on the total number of users, ratio of users to APs, and desired data rates.
- **Custom.** Use this option to specify a fixed number of APs.

The desired rate is selectable from 1 to 54 Mbps in both the Coverage and Capacity models.

Users

Note: The Users text boxes are active only when the Capacity model is selected.

- Enter the number of users you expect to have on your WLAN in the Users text box.
- Enter the number of users per AP you expect in the Users/AP text box.

The numbers entered in the these two text boxes must be non-zero integers between 1 and 255, inclusive.

Rates

Note: The Rate pull-down menus are active only when the Coverage or Capacity design models are selected.

Select the desired data rates from the pull-down menus for 802.11b/g and 802.11a.

High data transmission rates require an increased number of APs to be placed in your building. Carefully evaluate the data rate needs of your users.

AM Modeling Parameters Page

The AM Modeling Parameters page (Figure 4-6) allows you to specify the information necessary for RF Plan to determine the appropriate placement of your air monitors.

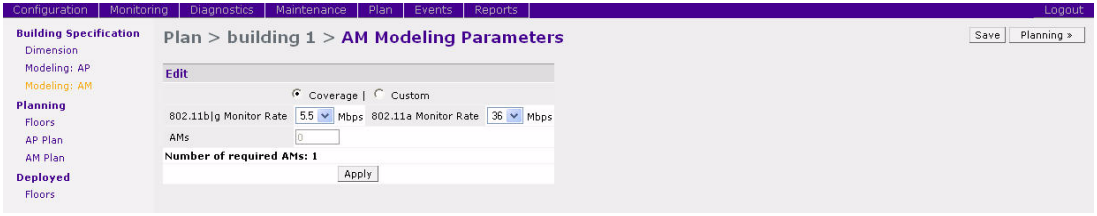

Figure 4-6

Controls on this page allow you to select the following functions, which are described in more detail in this section:

- **Design Model**. Use these radio buttons to specify a design model to use in the placement of AMs.
- **Monitor Rate**. Use this pull-down menu to specify the desired monitor rate for the AMs.
- **AMs.** Use this field to manually specify the number of AMs to deploy (Custom Model only).

Design Model

Two radio buttons on the page allow you to specify the model used to determine the number and type of AMs.

- **Coverage.** Use this option to let RF Plan automatically determine the number of AMs based on desired monitor rates and the configuration of the building.

  The desired rate is selectable from 1 to 54 Mbps in the Coverage model.

- **Custom.** Use this option to specify a fixed number of AMs. When the AM Plan portion of RF Plan is executed, RF Plan distributes the AMs evenly.

	**Note:** The monitor rates you select for the AMs should be less than the data rates you selected for the APs. If you set the rate for the AMs at a value equal to that specified for the corresponding PHY type AP, RF Plan allocates one AM per AP. If you specify a monitor rate greater than the data rate, RF Plan allocates more than one AM per AP.

Monitor Rates

Use the drop-down menus to select the desired monitor rates for 802.11b/g and 802.11a AMs.

	**Note:** This option is available only when the Coverage design model is selected.

Planning Floors Page

The Planning Floors page (Figure 4-7) enables you to see the footprint of your floors.

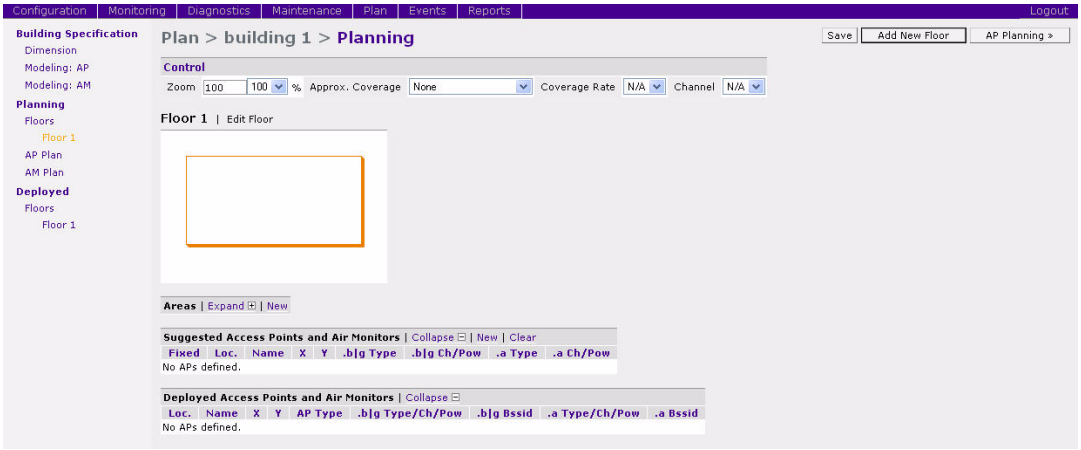

Figure 4-7

You can select or adjust the following features, which are described in more detail in this section:

- **Zoom.** Use this pull-down menu or type a zoom factor in the text field to increase or decrease the size of the displayed floor area.
- **Approximate Coverage Map**. Use this pull-down to select a particular radio type for which to show estimated coverage.
- **Coverage Rate.** Use this pull-down to modify the coverage areas based on a different data rate.
- **Edit Floor.** Click this link to launch the Floor Editor dialog box. See “Floor Editor Dialog Box” on page 4-12.
- **New in Areas section.** Click this link to launch the Area Editor dialog box. “Area Editor Dialog Box” on page 4-13.
- **New in Suggested Access Points and Air Monitors.** Click this link to launch the Suggested Access Point Editor dialog box. “Access Point Editor Page” on page 4-15.

Zoom

The Zoom control sets the viewing size of the floor image. It is adjustable in discrete steps from 10% to 1000%. You can either select a value from the pull-down zoom menu or specify a value in the text box to the left of the pull-down. When you specify a value, RF Plan adjusts the values in the pull-down to display a set of values both above and below the value you typed in the text box.

Coverage

Select a radio type from the Coverage pull-down menu to view the approximate coverage area for each of the APs that RF Plan has deployed in the AP Plan or AM Plan (Figure 4-8). Adjusting the Coverage values help you to understand how the AP coverage works in your building.

	Note: You will not see coverage areas displayed here until you have executed either an AP Plan or an AM Plan.

Figure 4-8

Coverage Rate

Adjusting the coverage rate also affects the size of the coverage areas for AMs. Adjusting the rate values helps you to understand how the coverage works in your proposed building.

Floor Editor Dialog Box

The Floor Editor dialog box (Figure 4-9) allows you to specify the background image and name the floor. The Floor Editor is accessible from the Floors Page by clicking on the Edit Floor link.

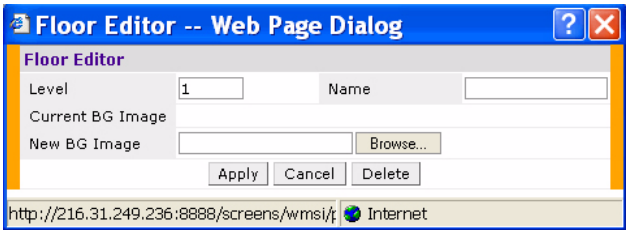

Figure 4-9

Naming. You can name the floor anything you choose as long as the name is an alphanumeric string with a maximum length of 64 characters. The name you specify appears to the right of the Floor Number displayed above the background image in the Planning view.

Background Images. You can import a background floor plan image into RF Plan for each floor. A background image is extremely helpful when specifying areas where coverage is not desired or areas where an AP or AM is not to be physically deployed.

Select a background image using the Browse button on the Floor Editor dialog box.

- **File Type and Size**. Background images must be JPEG format and cannot exceed 2048 x 2048 pixels in size. If you attempt to import a file with a larger pixel footprint, the image will not scale to fit the image area in the floor display area.

	Note: Because background images for your floors are embedded in the XML file that defines your building, minimize the file size of the JPEGs that you use for your backgrounds. You can minimize the file size by selecting maximum compression (lowest quality) in most graphics programs.

- **Image Scaling**. Images are scaled (stretched) to fit the display area. The display area aspect ratio is determined by the building dimensions specified on the Dimension page.

Area Editor Dialog Box

The Area Editor dialog box (Figure 4-10) allows you to specify areas on your building's floors where you either do not care about coverage, or where you do not want to place an AP or AM. You specify these areas by placing them on top of the background image using the Area Editor. Open the Area Editor dialog box by clicking New in the Areas section.

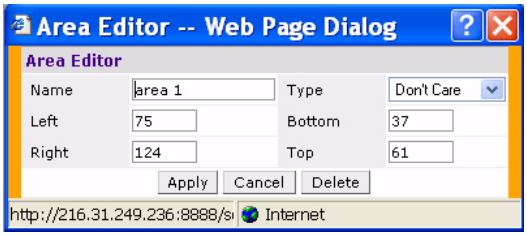

Figure 4-10

Naming. You can name an area using an alphanumeric string of characters with a maximum length of 64 characters. Give areas meaningful names so that they are easily identified.

Locating and Sizing. Specify absolute coordinates for the lower left corner and upper right corner of the box that represents the area you are defining. The datum for measurement is the lower left corner of the rectangular display area that represents your building's footprint. The coordinates of the upper right corner of the display area are the absolute (no unit of measure) values of the dimensions you gave your building when you defined it with the dimension feature.

Note: The location is zero-based. Values range from 0 to (height - 1 and width - 1). For example, if you defined your building to be 200 feet wide and 400 feet long, the coordinates of the upper right corner would be (199, 399).

Don't Care areas are displayed as orange rectangles (Figure 4-11) and Don't Deploy areas are displayed as yellow rectangles (Figure 4-12). You can drag your defined area to the location where you want it, and resize it by dragging one or more of the handles in the corners of the rectangle.

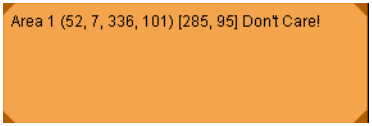

Figure 4-11

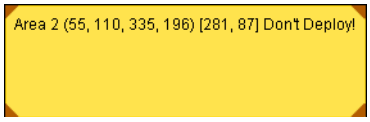

Figure 4-12

Access Point Editor Page

The Access Point Editor (Figure 4-13) allows you to manually create or modify a suggested AP.

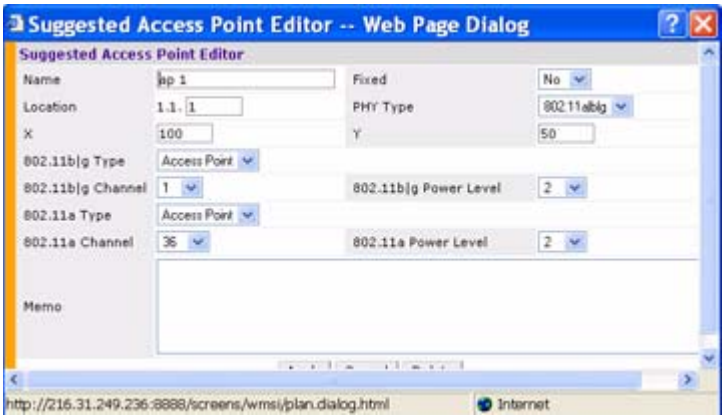

Figure 4-13

Naming. RF Plan automatically names APs using the default convention **ap** *number*, where *number* starts at 1 and increments by one for each new AP. When you manually create an AP, the new AP is assigned the next number and is added to the bottom of the suggested AP list.

You can name an AP anything you wish. The name must consist of alphanumeric characters and be 64 characters or less in length.

X and Y Coordinates. The physical location of the AP is specified by X-Y coordinates that begin at the lower left corner of the display area, as shown in Figure 4-14. The numbers you specify in the X and Y text boxes are whole units. The Y coordinate increases as a point moves up the display, and the X coordinate increases as it moves from left to right across the display.

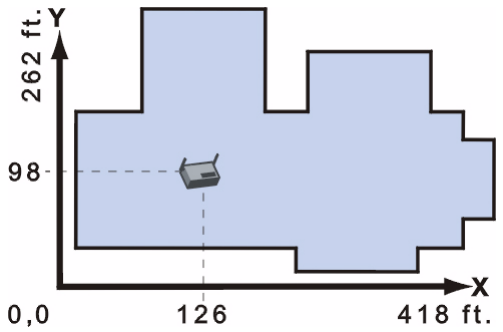

Figure 4-14

Fixed. Fixed APs do not move when RF Plan executes the positioning algorithm.

	Note: You would typically set a fixed AP when you have a specific room, such as a conference room, in which you want saturated coverage. Consider also using fixed APs for areas with unusually high user density.

Choose Yes or No from the drop-down menu. Choosing Yes locks the position of the AP as it is shown in the coordinate boxes of the Access Editor. Choosing No allows RF Plan to move the AP as necessary to achieve best performance.

PHY Types. The PHY Type drop-down menu allows you to specify what radio mode the AP uses. You can choose from one of the following:

- 802.11a/b/g
- 802.11a
- 802.1 b/g

802.11 Types. The 802.11 b/g and 802.11a Type drop-down menus allow you to choose the mode of operation for the AP. You can set the mode of operation to either Access Point or Air Monitor.

802.11 Channels. The 802.11a and 802.11b/g channel drop-down menus allow you to select from the available channels.

	Note: The channels available vary depending on the regulatory domain (country) in which the device is being operated.

- 802.11a channels begin at channel 34 at a frequency of 5.170 MHz and increase in 20-MHz steps through channel 161 at 5.805 Mhz.
- 802.11b/g channels begin at 1 and are numbered consecutively through 14. The frequencies begin at 2.412 MHz on channel 1 and increase in 22-MHz steps to Channel 14 at 2.484 MHz.

802.11 Power Levels. The power level drop-down menus allow you to specify the transmission power of the AP. Choices are OFF, 0, 1, 2, 3, and 4. A setting of 4 applies the maximum Effective Isotropic Radiated Power (EIRP) allowed in the regulatory domain (country) in which you are operating the AP.

Memo. The Memo text field allows you to enter notes regarding the AP. You can enter a maximum of 256 alphanumeric characters in the Memo field.

AP Planning Page

The AP Planning page (Figure 4-15) uses the information entered in the modeling pages to locate access points in the buildings you described.

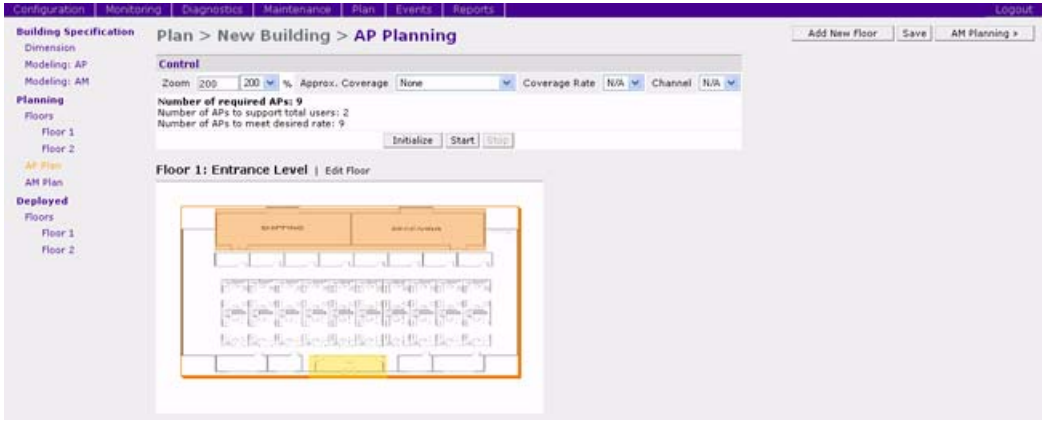

Figure 4-15

Initialize

Initialize the optimizing algorithm by clicking the Initialize button. This makes an initial placement of the APs and prepares RF Plan for the task of determining the optimum location for each AP. As soon as you click Initialize, you will see the AP symbols appear on the floor plan.

Colored circles around the AP symbols (shown in Figure 4-16) indicate the approximate coverage of the individual AP, and the color of the circle represents the channel on which the AP is operating. The circles appear after you select an *approximate coverage* value on one of the Floors pages. You can also click an AP icon and drag it to manually reposition it.

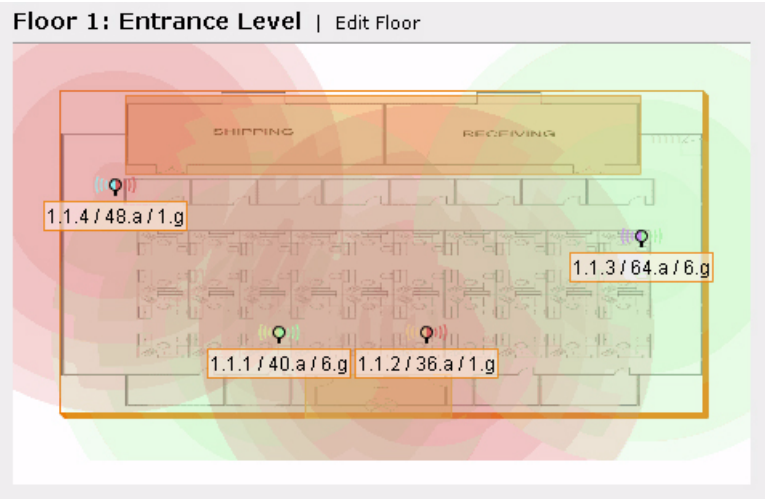

Figure 4-16

Start

Click Start to launch the optimizing algorithm. The AP symbols move on the page as RF Plan finds the optimum location for each.

The process may take several minutes. You can watch the progress on the status bar of your browser. The algorithm stops when the movement is less than a threshold value calculated based on the number of APs. The threshold value is also displayed in the status bar at the bottom of the browser window.

	Note: IRM scanning must be enabled for the AP and AM plans to work properly. Enable IRM in the configuration > advanced > radio > page for all the radios.

Viewing the Results

You can view the results of optimizing algorithm two ways: graphically and in a table of suggested APs. To obtain information about a specific AP, place the cursor over its symbol. An information box appears (Figure 4-17) containing information about the AP's exact location, PHY type, channel, power, and so on.

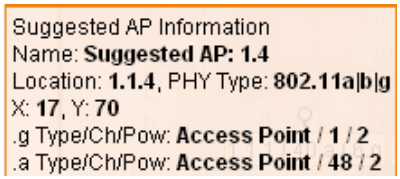

Figure 4-17

The Suggested Access Points and Air Monitors table (Figure 4-18) lists the coordinates, power, location, power setting, and channel for each of the APs shown in the floor plan.

Suggested Access Points and Air Monitors | Collapse ⊟ | New | Clear

Fixed	Loc.	Name	X	Y	.b|g Type	.b|g Ch/Pow	.a Type	.a Ch/Pow
No	1.1.1	Suggested AP: 1.1	68	24	Access Point	6 / 2	Access Point	40 / 2
No	1.1.2	Suggested AP: 1.2	114	24	Access Point	1 / 2	Access Point	36 / 2
No	1.1.3	Suggested AP: 1.3	181	54	Access Point	6 / 2	Access Point	64 / 2
No	1.1.4	Suggested AP: 1.4	17	70	Access Point	1 / 2	Access Point	48 / 2

Figure 4-18

AM Planning Page

The AM Planning page calculates the optimum placement for the air monitors.

Initialize

Initialize the algorithm by clicking Initialize. This makes an initial placement of the AMs and prepares RF Plan for the task of determining the optimum location for each of the AMs. When you click Initialize, the AM symbols appear on the floor plan.

Start

Click Start to launch the optimizing algorithm. The AM symbols move on the page as RF Plan finds the optimum location for each.

The process may take several minutes. Progress is displayed on the status bar of your browser. The algorithm stops when the movement is less than a threshold value calculated based on the number of AMs. The threshold value is also displayed in the status bar at the bottom of the browser window.

Viewing the Results

Viewing the results of the AM Planning feature is similar to that for the AP Planning feature.You can view the results of the optimizing algorithm two ways: graphically and in a table of suggested

AMs. To obtain information about a specific AM, place the cursor over its symbol. An information box appears (Figure 4-19), containing information about the AM's exact location, PHY type, channel, power, and so on.

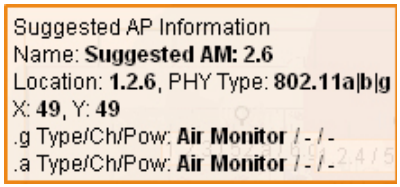

Figure 4-19

The Suggested Access Points and Air Monitors table (Figure 4-20) lists the coordinates, power, location, power setting, and channel for each of the AMs that are shown in the floor plan.

Figure 4-20

Exporting and Importing Files

The Export and Import buttons on the Building List page allow you to export and import files that define the parameters of your buildings. You can export a file so that it can be imported into and used to automatically configure a WFS709TP. On a WFS709TP, you can import a file that has been exported from another WFS709TP or from the standalone version of RF Plan that runs as a Windows application.

The files that you export and import are XML files and, depending on how many floors are in your buildings and how many background images you have for your floors, they can be quite large. (See "Background Images" on page 4-13.)

Export Buildings Page

To export a file that defines the parameters of one or more buildings, select the buildings to be exported in the Building List page and then click Export (Figure 4-21).

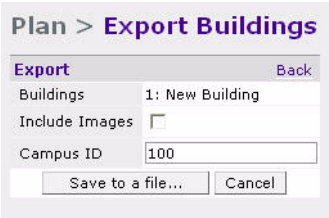

Figure 4-21

When exporting a building file, NETGEAR recommends that you select the Include Images checkbox.

When you click the Save to a file... button, you are prompted for the location and name for the exported file. Be sure to give the file the.XML file extension, for example, My_Building.XML.

Import Buildings Page

You can import only XML files exported from another WFS709TP or from the standalone version of RF Plan that runs as a Windows application.

Importing any other file, including XML files from other applications, might result in unpredictable results.

To import a file that defines the parameters of one or more buildings, click the Import button in the Building List page (Figure 4-22).

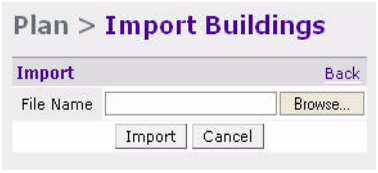

Figure 4-22

In the Import Buildings page, click Browse to select the file to be imported, then click the Import button.

Locate

The Locate button on the Building List page allows you to search for APs or AMs on a building-by-building basis. To use this feature, select the building in which you want to search, and click Locate.

The Deployed Access Points and Air Monitors table displays information on each of these devices.

- To add a device, click Add Device.
- To delete a device, click Remove Device.
- To select a device, click Choose Devices.

RF Plan Example

This section guides you through the process of creating a building and using RF Plan to populate it with APs and AMs.

Sample Building

The following planning summary shows the information to be used in this example.

Table 4-2.

Building Dimensions	
Height: *100*	Width: *100*
Number of Floors: *2*	
User Information	
Number of Users:	Users per AP: *N/A*
Radio Types: *a,. b, g*	
Overlap Factor: *Medium (150%)*	
AP Desired Rates	
802.11b|g: *48 Mbps*	802.11a: *48 Mbps*
AM Desired Rates	
802.11b|g: *24*	802.11a: *24*
Don't Care/Don't Deploy Areas:	
Shipping & Receiving = Don't Care	
Lobby = Don't Deploy	

Create a Building

In this section you create a building using the information supplied in the planning summary.

1. Click New Building.

   The Overview page appears.

2. Click Save.

3. Click Building Dimension.

   The Specification page appears.

4. Enter the information shown in Table 4-3 into the text boxes (Figure 4-23).

Table 4-3. Building Planning Specifications

Text Box	Information
Building ID	1
Building Name	My building
Width	100
Length	100
Inter Floor Height	20
Units	Feet
Floors	2

Figure 4-23

5. Click Save.

6. Click Apply.

   RF Plan automatically moves to the next page in the list. In this case RF Plan moves to the AP Modeling Parameters page.

Model the Access Points

You now determine how many APs are required to cover your building with a specified data transfer rate and overlap.

In this example, you use the Coverage Model. The following assumptions are made about the performance of the WLAN:

- Radio Types: a/b/g
- Overlap factor: Medium (150%)
- 802.11a desired rate: 48 Mbps
- 802.11b desired rate: 48 Mbps

To model the access points:

1. Select 801.11 a|b|g from the Radio Type drop-down menu.
2. Select Medium from the Overlap Factor drop-down menu.

   Notice that the percentage show at the left of the drop-down menu changes to 150%.
3. Select 48 from the 802.11 b|g Desired Rate drop-down menu.
4. Select 48 from the 801.11 a Desired Rate drop-down menu.

   Notice that the number of required APs has changed to 9. (Figure 4-24)

Figure 4-24

5. Click Save, then Apply.

   RF Plan moves to the AM Modeling Parameters page.

Model the Air Monitors

You now determine how many AMs are required to provide a specified monitoring rate. In this example you continue to use the Coverage Model and make the following assumptions:

- 802.11 b|g monitor rate: 48 Mbps
- 802.11 a monitor rate: 48 Mbps

To model the air monitors:

1. Select 24 from the 802.11 b|g Monitor Rate drop-down menu.
2. Select 24 from the 802.11 a Monitor Rate drop-down menu.

   Notice that the number of required AMs is now 3. (Figure 4-25)

Figure 4-25

3. Click Save, then Apply.

   RF Plan moves to the Planning page.

Add and Edit a Floor

You now add floor plans to your floors (Figure 4-26). In this section you:

- Add a background image floor plan for each floor
- Name the floors

	Note: This section uses example floor plans that are provided with the Windows application version of RF Plan.

To add the background image and name the first floor:

1. In the Planning page, click the Edit Floor link at the right of the Floor 1 indicator.

2. Type **Entrance Level** in the Name box of the Floor Editor Dialog.
3. Use the Browse button to locate the background image for the first floor.
4. Click Apply.

To add the background image and name the second floor:

1. Click the Edit Floor link at the right of the Floor 2 indicator.
2. Type **Second Level** in the Name box of the Floor Editor Dialog.
3. Use the Browse button to locate the background image for the second floor.
4. Click Apply.
5. Click Save on the Planning page.

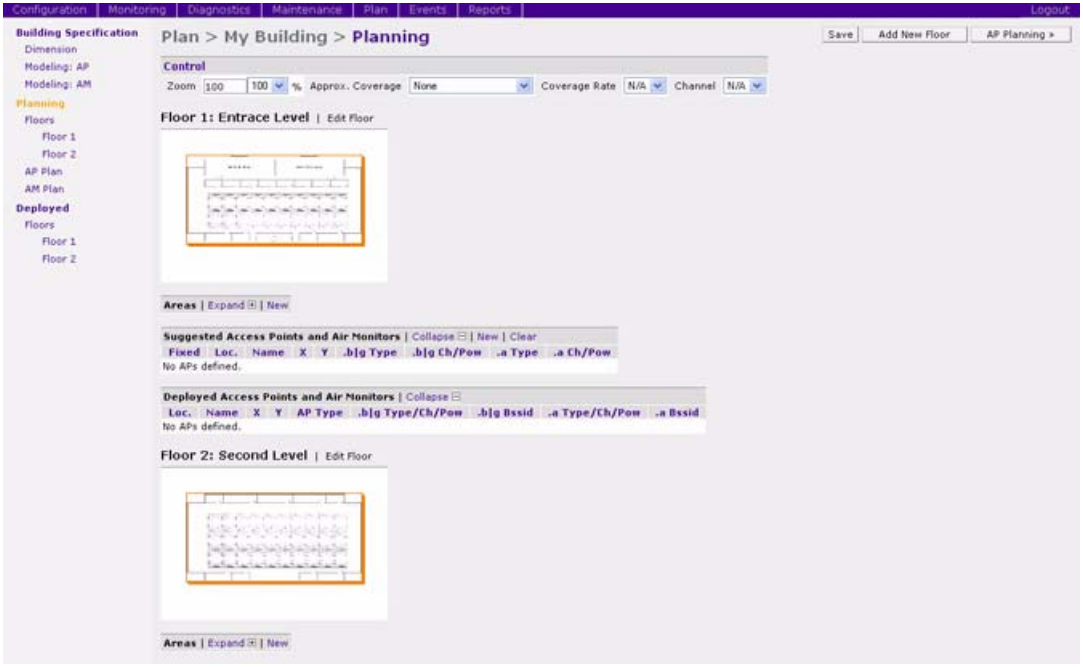

Figure 4-26

Defining Areas

Before you advance to the AP and AM Planning pages, you want to define special areas where you do not want to physically deploy an AP or AP, or where you do not care if there is coverage or not.

This example assumes the following:

- You do not care if you have coverage in the Shipping and Receiving areas.
- You do not want to deploy APs or AMs in the Lobby Area.

Create a Don't Care Area

To create a Don't Care area:

1. Click AP Plan in the Feature Tree at the left side of the browser window.

> **Note:** You can zoom in on the floor plan using the Zoom pull-down near the top of the AP Planning page, or type a zoom value in the text box at the left of the pull-down and press the enter key on your keyboard.

2. In the Planning page, click the New link in the Areas section under Floor 1.

   This opens the Area Editor.

3. Type **Shipping and Receiving** in the Name text box in the Area Editor.
4. Select Don't Care from the Type pull-down menu box.
5. Click Apply.

   An orange box appears near the center of the floor plan.

   The information you typed in the editor appears in the box. You see the name and type of area, as well as the coordinates of the lower left corner and upper right corner of the box.

> **Note:** The x = 0 and y = 0 coordinates correspond to the lower left corner of the layout space.

6. Using your mouse, click and drag the box over the Shipping and Receiving area.
7. Drag one corner of the box to a corresponding corner of the Shipping and Receiving area and using one of the corner handles of the box, stretch it to fit exactly over the Shipping and Receiving area.

   Your floor plan with the Don't Care box should look similar to Figure 4-27.

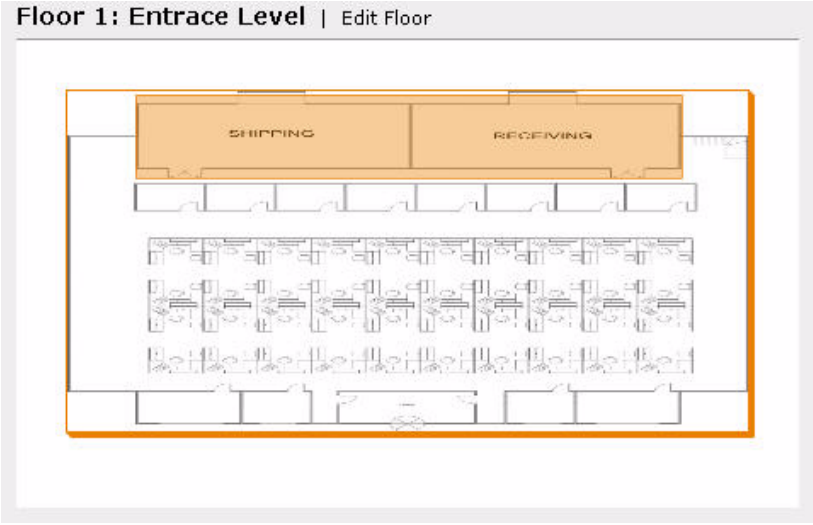

Figure 4-27

8. Click Save.

Create a Don't Deploy Area

To create a Don't Deploy area:

1. Click the New link in the Areas section under Floor 1 to open the Area Editor.
2. Type Lobby in the Name text box in the Area Editor.
3. Select Don't Deploy from the Type pull-down menu box.
4. Click Apply.

   An yellow box appears near the center of the floor plan.

   The information you typed in the editor appears in the box. You see the name and type of area, as well as the coordinates of the lower left corner and upper right corner of the box.

> **Note:** The x = 0 and y = 0 coordinates correspond to the lower left corner of the layout space.

5. Using your mouse, click and drag the box over the Lobby area on the floor plan.

6. Drag one corner of the box to a corresponding corner of the lobby and using one of the corner handles of the box, stretch it to fit exactly over the lobby area.

   Your floor plan with the Don't Deploy box added should look similar to Figure 4-28.

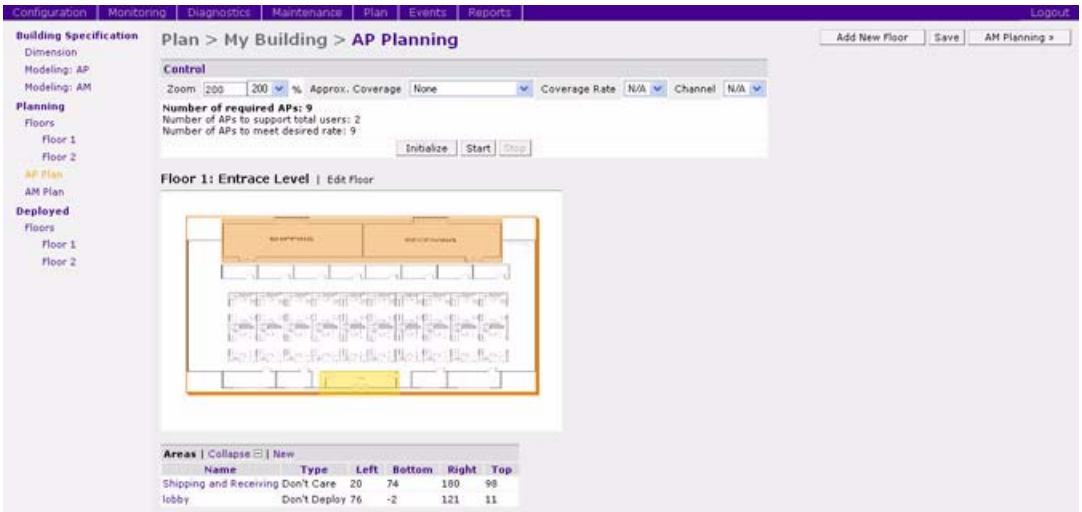

Figure 4-28

7. Click Save.

Running the AP Plan

In this section you run the algorithm that searches for the best place to put the APs.

To zoom in on the floor plan, use the Zoom pull-down near the top of the AP Planning page, or type a zoom factor in the text box at the left of the pull-down and press the Enter.

Notice that the number of required APs is nine, the same value that you saw when you modeled your APs. Notice also that none of the APs show on the floor plan yet.

1. Click Initialize.

   A total of nine AP symbols appears on the two floor diagrams: four on Floor 1 and five on Floor 2. The Suggested Access Points tables below each floor diagram have also been populated with information about the suggested APs for each corresponding floor.

2. Click Start.

   After you initialize the APs, you must start the algorithm. The APs move around on the floor plans as the algorithm is running.

The algorithm stops when the movement is less than a threshold value calculated based on the number of APs. The threshold value is displayed in the status bar at the bottom of the browser window.

Note: To see the approximate coverage areas of each of the APs, select an AP type from the Approx. Coverage pull-down box and select a rate from the Coverage Rate pull-down box.

The result should look similar to Figure 4-29.

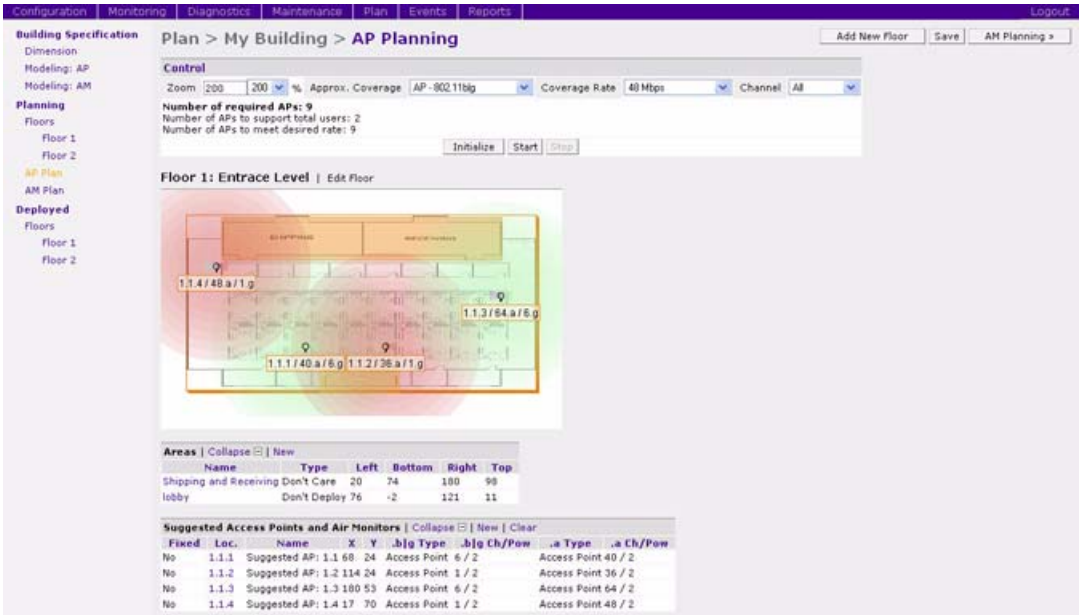

Figure 4-29

3. Click Save, then click AM Planning.

Running the AM Plan

Running the AM Plan algorithm is similar to running the AP Plan.

1. Click Initialize then Start.

   The algorithm stops when the movement is less than a threshold value calculated based on the number of AMs. The threshold value is displayed in the status bar at the bottom of the browser window.

2. Click Save.

Chapter 5
Configuring WLANS

This chapter explains how to configure a wireless LAN (WLAN) using the browser interface. It includes the following topics:

Before You Begin

This section describes tasks that you need to do prior to configuring a WLAN.

You have a wide variety of options for authentication, encryption, access management, and user rights when you configure a WLAN with a WFS709TP ProSafe Smart Wireless Switch. However, you *must* configure the following basic elements:

- A Service Set Identifier (SSID) that uniquely identifies the WLAN.
- Layer 2 authentication to protect against unauthorized access to the WLAN. The authentication method you choose determines the following:
  - Layer 2 encryption to ensure the privacy and confidentiality of the data transmitted to and from the network.
  - An authentication server used to validate the user. Authentication can be performed using an external authentication server, such as a RADIUS server, or the WFS709TP's internal database.
- A virtual local area network (VLAN) on the WFS709TP into which wireless clients who successfully associate to the access point (AP) are placed.

Determine the Authentication Method

A user must authenticate to the system in order to access WLAN resources. Table 5-1 describes the types of authentication that you can configure for a WLAN.

Table 5-1. Authentication Methods

Method	Description
None (also called open system authentication)	This is the default authentication protocol. The client's identity, in the form of the media access control (MAC) address of the wireless adapter in the wireless client, is passed to the WFS709TP. Essentially, any client requesting access to the WLAN is authenticated.
IEEE 802.1x	The IEEE 802.1x authentication standard allows for the use of keys that are dynamically generated on a per-user basic (as opposed to a static key that is the same on all devices in the network). The 802.1x standard requires the use of a RADIUS authentication server. Most Lightweight Directory Access Protocol (LDAP) servers do not support 802.1x.
Wi-Fi Protected Access (WPA)	WPA implements most of the IEEE 802.11i standard. It is designed for use with an 802.1x authentication server (the Wi-Fi Alliance refers to this mode as WPA-Enterprise). WPA uses the Temporal Key Integrity Protocol (TKIP) to dynamically change keys and RC4 stream cipher to encrypt data.
WPA in pre-shared key (PSK) mode (WPA-PSK)	With WPA-PSK, all clients use the same key (the Wi-Fi Alliance refers to this mode as WPA-Personal). In PSK mode, users must enter a passphrase from 8-63 characters to access the network. PSK is intended for home and small office networks where operating an 802.1x authentication server is not practical.
WPA2	WPA2 implements the full IEEE 802.11i standard. In addition to WPA features, WPA2 provides Counter Mode with Cipher Blocking Chaining Message Authentication Code Protocol (CCMP) for encryption that uses the Advanced Encryption Standard (AES) algorithm. (The Wi-Fi Alliance refers to this mode as WPA2-Enterprise.)
WPA2-PSK	WPA2-PSK is WPA2 used in PSK mode, where all clients use the same key. (The Wi-Fi Alliance refers to this mode as WPA2-Personal.)
Captive Portal	Captive Portal allows users to authenticate using a web-based portal. Captive Portal users can be authenticated to an external authentication server or to the internal database on the WFS709TP. Captive Portal authentication does not provide any type of data encryption beyond the SSL encryption used during the authentication. You can configure WEP encryption or WPA-PSK, or WPA2-PSK authentication in conjunction with Captive Portal.
MAC	Allows the media access control (MAC) address of a device to be authenticated to an external authentication server or to the internal database on the WFS709TP. You can configure MAC authentication in conjunction with WPA-PSK or WPA2-PSK authentication.

The Layer 2 encryption depends upon the authentication method chosen (Table 5-2).

Table 5-2. Encryption Options by Authentication Method

Authentication Method	Encryption Option
None	Open (Null) or Static WEP
802.1x	Dynamic WEP
WPA or WPA-PSK	TKIP
WPA2, WPA2-PSK, or xSec	AES
Combination of WPA or WPA-PSK and WPA2 or WPA2-PSK	Mixed TKIP/AES

For more information about data encryption options for the WLAN, see "Encryption" on page 1-10.

Authentication Server

If an external authentication server, such as a RADIUS server, will be used to validate the wireless user, the server administrator must configure the server to support this authentication. The administrator must also configure the server to allow communication with the WFS709TP.

If the internal database in the WFS709TP will be used to validate the wireless user, you must configure user entries in the database.

Table 5-3 is a summary of the authentication servers that you can configure for each authentication type in your WLAN.

Table 5-3. Supported Authentication Servers by Authentication Types

Authentication Type	Authentication Servers		
	RADIUS	LDAP	Internal DB
802,1x	Yes	Yes**	Yes*
WPA	Yes	Yes**	Yes*
WPA-PSK	N/A	N/A	N/A
WPA2	Yes	Yes**	Yes*
WPA-PSK2	N/A	N/A	N/A
Captive Portal	Yes	Yes	Yes
MAC	Yes	Yes	Yes

* Only when the AAA FastConnect feature is enabled. See "Configuring 802.1x Authentication" on page 7-4.

** Only when the AAA FastConnect feature is enabled and EAP-Generic Token Card (EAP-GTC) is used within the Protected EAP tunnel. See "Configuring 802.1x Authentication" on page 7-4.

Determine the Default VLAN

Each SSID is linked to a VLAN on the WFS709TP. Successful wireless client association to an AP places the user into the default VLAN specified by the SSID configuration. The default VLAN can be overridden by authentication server attributes; if you are authenticating a user to an external authentication server, the user VLAN can be based on attributes returned by the server during authentication.

Basic WLAN Configuration in the Browser Interface

The WLAN Basic Configuration page in the browser interface allows you to define many useful options that pertain to a specific SSID without having to navigate to other configuration pages. These options include:

- SSID
- Radio type: 802.11a, 802.11b/g, or 802.11a/b/g
- Layer 2 authentication and encryption type
- "Advanced" authentication features such as Captive Portal, VPN, and MAC authentication, in addition to Layer 2 authentication
- Authentication server: either RADIUS or the WFS709TP's internal database

Note: If the authentication server is a RADIUS server, you can configure server parameters on the WLAN Basic Configuration page

- VLAN into which wireless clients are placed

When you configure a WLAN in the WLAN Basic Configuration page, the SSID will not be hidden in beacons sent by the AP. In addition, the system does not send the SSID in response to broadcast probe requests sent by clients.

Note the following about using the WLAN Basic Configuration page:

- The SSID configuration is global, that is, it applies to all APs in the network. If you need to configure a WLAN for a set of APs in a specific location—for example, a WLAN that only applies to a particular building or floor—you must configure the SSID using the WLAN Advanced Configuration pages.

- You can assign only one VLAN to the SSID. If you need to have multiple VLANs configured for a WLAN, you must configure the SSID using the WLAN Advanced Configuration pages.
- The authentication server must be a RADIUS server or the WFS709TP's internal database.

  If you specify a RADIUS server, you can configure the server's IP address, authentication and accounting ports, and shared key.

> **Note:** The RADIUS server administrator must configure the server for communication with the WFS709TP.

  If you specify the WFS709TP's internal database, you will need to navigate to the Configuration > Advanced > Security > Authentication Servers > Internal DB to add entries to the database.

To configure an SSID in the WLAN Basic Configuration page, navigate to the Configuration > Basic > WLAN page (Figure 5-1).

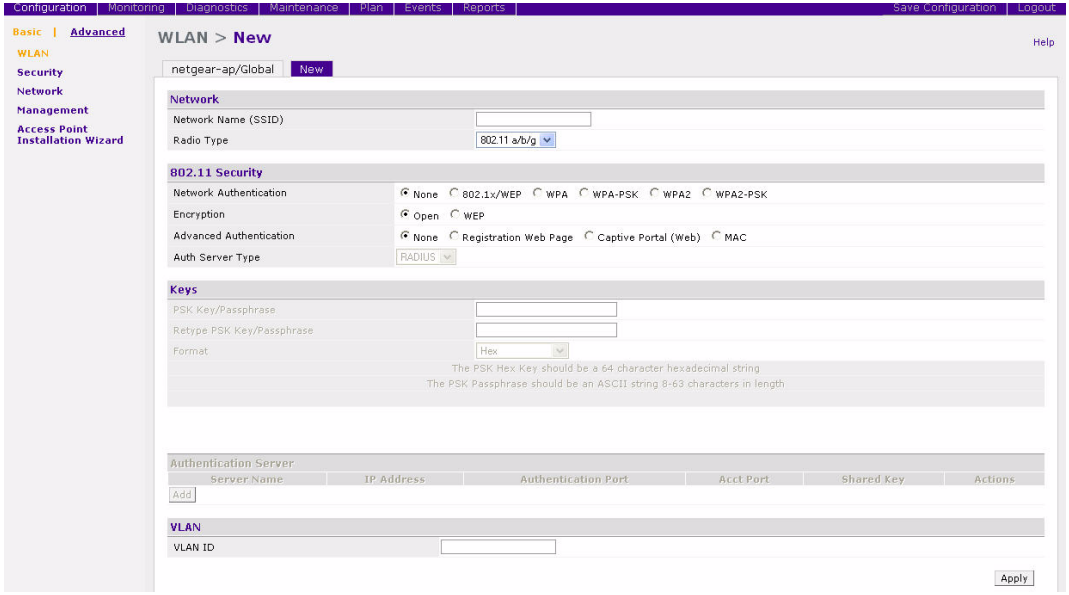

Figure 5-1

Table 5-4 describes the options available from the WLAN Basic Configuration page.

Table 5-4. WLAN Basic Configuration Parameters

Parameter	Definition
Network Section:	
Network Name (SSID)	A name that uniquely identifies the WLAN.
Radio Type	The radio type on which this SSID is configured: 802.11a only, 802.11b/g only, or 802.11a/b/g
802.11 Security:	
Network Authentication	The Layer 2 security mechanism used to protect unauthorized access to the WLAN. See "Determine the Authentication Method" on page 5-2.
Encryption	The Layer 2 encryption used on the WLAN to ensure the privacy and confidentiality of the data transmitted to and from the network. The encryption type is dependent upon the type of network authentication selected.
Advanced Authentication	The default is None, however, you can select one of the following methods: • Registration Web Page: Allows users to access the WLAN using a web-based portal. Users typically enter an email address as an identification but are not authenticated. • Captive Portal (Web): Allows users to authenticate using a web-based portal. Captive Portal requires users to be authenticated to an external authentication server or to the internal database on the WFS709TP. • MAC: Allows the media access control (MAC) address of a device to be authenticated to an external authentication server or to the internal database on the WFS709TP. You can select one of the Advanced Authentication methods only if the Network Authentication is None, WPA-PSK, or WPA2-PSK.
Auth Server Type	Either the internal database or an external RADIUS server. Activated only if 802.1x/WEP, WPA, WPA2, xSec, Captive Portal, VPN, or MAC authentication is configured.
Keys	Configures the static WEP key or TKIP key for WPA-PSK or WPA2-PSK authentication. (Activated only if static or PSK-based security options are configured.) • For Static WEP, enter either a 10-hexadecimal digit key or a 26-hexadecimal digit key. • For TKIP, enter either a 64-character hexadecimal string or an 8-63 character ASCII passphrase.

Table 5-4. WLAN Basic Configuration Parameters (continued)

Parameter	Definition
Authentication Server	Configures the RADIUS authentication server. (Activated only if the authentication requires an authentication server and the server type is RADIUS.) If you have previously configured a RADIUS authentication server, select the server from the drop-down list. To configure a RADIUS server, click New and enter the following information: • Server name • IP address of the server • Authentication port • Accounting port • Shared key Click Add when you are done. The information for the server appears. If you are using an LDAP server or internal database for authentication, you need to configure the authentication server by navigating to the Configuration > Advanced > Security > AAA Servers page.
VLAN	Specifies the user VLAN for wireless clients that associate to the SSID.

Example Configuration

This section describes how to use the WLAN Basic Configuration page to configure a WLAN to provide network access for company employees who use wireless PCs. Employees are typically validated against a corporate database on an authentication server before they are allowed access to the network. Once validated, users are placed into a specified VLAN on the corporate network.

In this example, the WLAN has the following characteristics:

- SSID: corpnet
- Radio Type: 802.11 b/g
- Authentication: WPA
- Encryption: KIP
- VLAN: 10

A RADIUS server is used to authenticate users. The following is the RADIUS server information for this example:

- Server Name: RadiusO1
- IP Address: 0.3.22.253
- Authentication Port: 1812
- Acct Port: 1813

- Shared Key: radius123

The administrator for the RADIUS server must configure the server to support authentication. The administrator must also configure the server to allow communication with the WFS709TP.

To configure the WLAN in the WLAN Basic Configuration page:

1. Navigate to the Configuration > Basic > WLAN page. Enter corpnet for Network Name (SSID).
2. Select 802.11 b/g for Radio Type.
3. Select WPA for Network Authentication

   TKIP is automatically selected for the encryption and Auth Server Type is activated with RADIUS selected.
4. Under Authentication Server, click Add.
5. Under Choose an Authentication Server, select NEW and click Add.
   a. Enter Radius01 for Server Name.
   b. Enter 10.3.22.253 for IP Address.
   c. Enter radius123 for Shared Key.
   d. Click Add. The server information appears under Authentication Server.
6. Enter 10 for VLAN ID.

   The page should look like Figure 5-2.

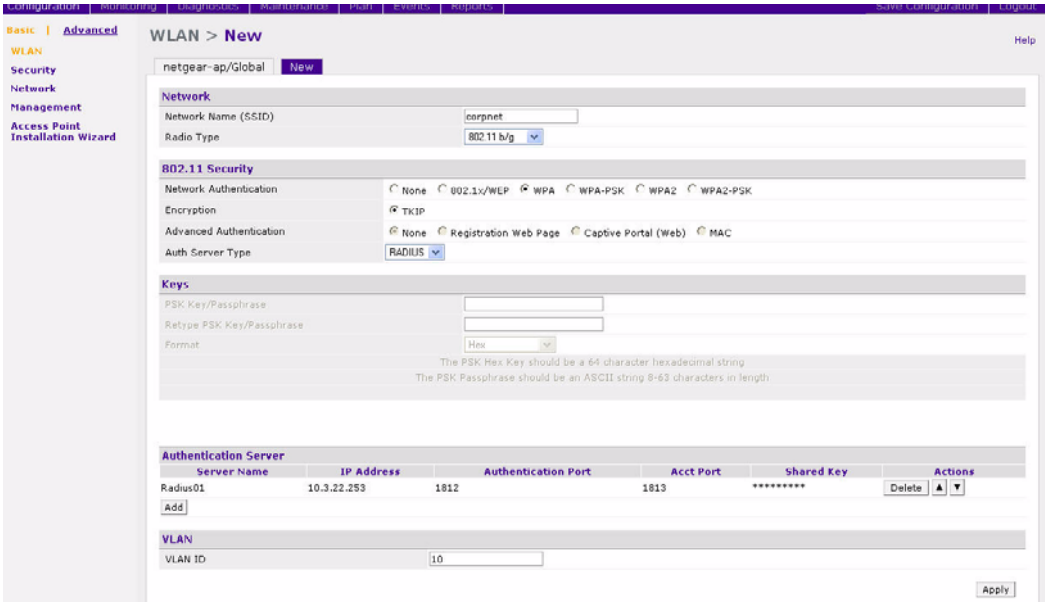

Figure 5-2

7. Click Apply.

Advanced WLAN Configuration in the Browser Interface

The Advanced WLAN configuration pages allow you to configure the following features:

- Global SSID and radio parameters that affect all APs in the network
- SSID and radio parameters for APs in specific locations in the network

The parameters that you configure for global or location-specific SSID and radio configurations are identical. However, if the same parameters are configured for global and location-specific APs for a WLAN, the location-specific values override global values.

For example, if you set the maximum number of clients to 30 in the global configuration for WLAN-01 and set the maximum number of clients to 15 for location 1.2.1 for the same SSID, the APs in location 1.2.1 will have a maximum of 15 clients.

Configuring Global Parameters

To configure global parameters that affect all APs in the network:

- Navigate to the Configuration > Advanced > WLAN > Network > SSID page to add or modify SSIDs.
- Navigate to the Configuration > Advanced > WLAN > Network > General page to configure or modify AP parameters.
- Navigate to the Configuration > Advanced > WLAN > Radio page to configure radio settings.

Configuring Location-Specific Parameters

To configure parameters that only affect APs in specific locations in the network:

1. Navigate to the Configuration > Advanced > WLAN > Advanced page.
2. Click Add to add a new location.
3. Enter a location ID in the format *building.floor.plan*, where each value is an integer.
4. Click Add.
5. (Optional) Customize the configuration of the specified location.
   - Select the SSID tab to add or modify SSIDs.
   - Select the General tab to configure AP parameters.
   - Select the 802.11b/g or 802.11a tab to configure radio settings.

Note: The global pages and location-specific configuration tabs contain identical configuration parameters, which are described in the following sections. Remember that location-specific values override global values for the same parameters.

Add or Modify SSIDs

You can configure 802.11 settings for an SSID in the Basic or Advanced WLAN configuration pages. The Advanced WLAN pages also allow you to configure additional SSID settings that are not available in the Basic configuration page; these settings are described later in this section.

To add or modify an SSID that affects all APs in the network

1. Navigate to the Configuration > Advanced > WLAN > Network > SSID page.
2. Select whether you want to add a new SSID or modify an existing SSID,
   - To add a new SSID, click Add.
   - To edit an existing SSID click Edit.

The SSID configuration page appears.

To add or modify an SSID for APs in a specific location in the network:

1. Navigate to the Configuration > Advanced > WLAN > Advanced page (Table 5-3).
2. Click Add to add a new location.
3. Enter a location ID in the format building.floor.plan, where each value is an integer.
4. Click Add.
5. Select the SSID tab to add or modify SSIDs.

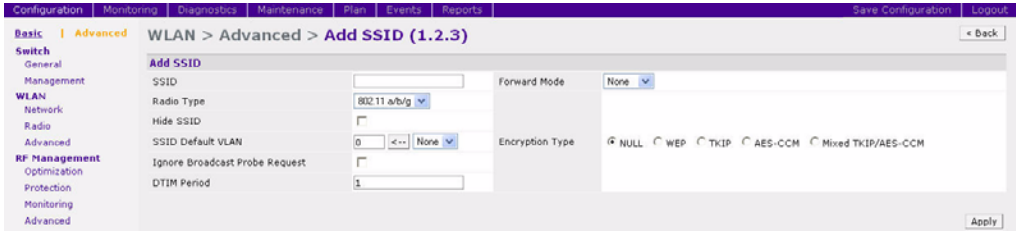

Figure 5-3

Default SSID

The default SSID is **netgear-ap**. This will be broadcast as a valid SSID if the value is not changed. This is the only SSID that permits a name change. To change the name of other SSIDs but retain the configurations:

1. Create a new SSID with the desired name and settings.
2. Delete the existing SSID entry.

Advanced SSID Configuration Settings

The SSID configuration in the Advanced WLAN pages allow you to configure the following SSID settings that are not available in the Basic configuration page:

- **Forward Mode.** Controls whether 802.11 frames are tunneled to the WFS709TP using Generic Routing Encapsulation (GRE), or bridged into the local Ethernet LAN.

  This setting can also be configured on a per-radio basis in the radio settings pages.

- **Hide SSID.** Enables or disables hiding of the SSID name in beacon frames.

  This setting can also be configured on a per-radio basis in the radio settings pages.

- **Ignore Broadcast Probe Request.** When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients must know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.

  This setting can also be configured on a per-radio basis in the radio settings pages.

- **DTIM Period.** Specifies the interval between the sending of Delivery Traffic Indication Messages (DTIMs) in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed. When using wireless clients that employ power management features to sleep, the client must revive at least once during the DTIM period to receive broadcasts. The default is 2.

  This setting can also be configured on a per-radio basis in the radio settings pages.

- **Mixed TKIP/AES-CCM encryption.** Selecting this option displays additional selections:

  - PSK TKIP/AES-CCM for static TKIP and AES key configuration
  - WPA/2 TKIP/AES-CCM for dynamic TKIP and AES

  If you select PSK TKIP/AES-CCM, the key can be hex or ASCII. Enter a 64-character hex key or an 8-character to 63-character ASCII key.

Configure AP Information

Use the General configuration in the Advanced WLAN pages to configure AP logging and debugging, Simple Network Management Protocol (SNMP) system information and trap receivers, and other information.

- To configure information that applies to all APs in the network, navigate to the Configuration > Advanced > WLAN > Network > General page (Figure 5-4).

To configure information that applies to APs in a specific location in the network:

1. Navigate to the Configuration > Advanced > WLAN > Advanced page.
2. Click Add to add a new location.
3. Enter a location ID in the format building.floor.plan, where each value is an integer.
4. Click Add.
5. Select the General tab.

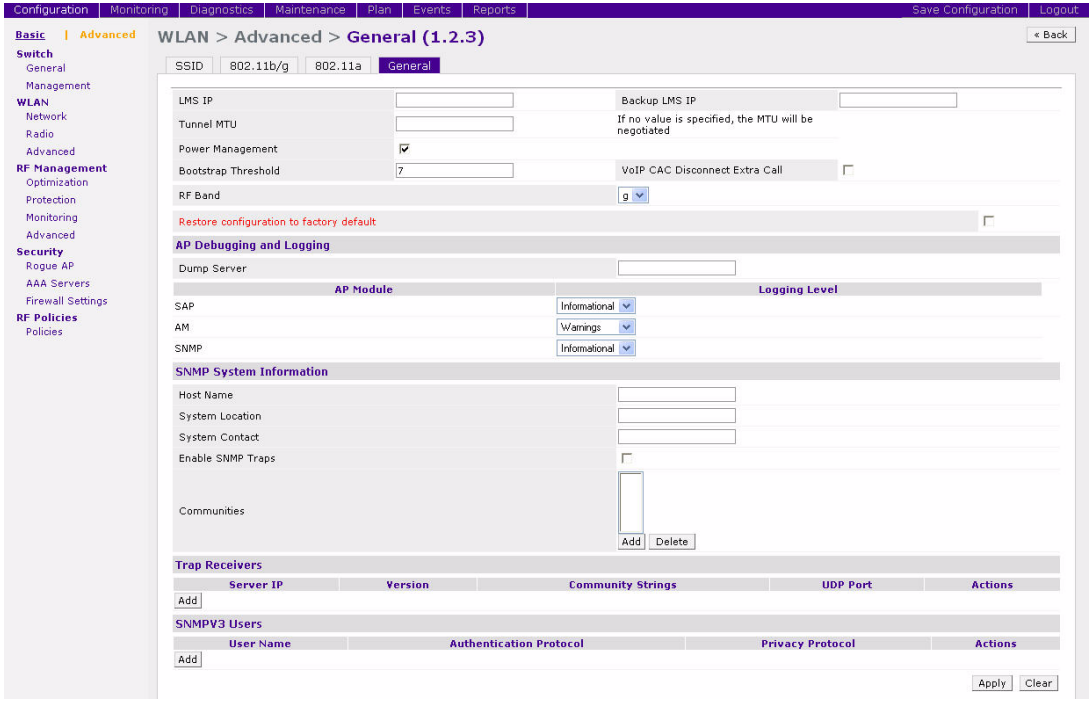

Figure 5-4

The General configuration in the Advanced WLAN pages allows you to configure the following settings:

- **LMS IP and Backup LMS IP.** Specifies the local management switch (LMS) that the AP uses in multi-switch networks. The LMS is responsible for terminating user traffic from the APs, processing it, and forwarding it to the wired network. An AP can boot up from any WFS709TP on the WLAN network (in a setup with master and local WFS709TPs), if all of the WFS709TPs are on the same VLAN and if load balancing is enabled on the WFS709TP. To force the AP to boot with a particular WFS709TP, configure the LMS IP with the address of the desired WFS709TP.

  When using redundant switches as the LMS, set this parameter to be the Virtual Router Redundancy Protocol (VRRP) IP address to ensure that APs always have an active IP address with which to terminate sessions.

- **Tunnel MTU.** Maximum transmission unit (MTU) size of the wired link for the AP. If no value is specified, the MTU size is negotiated.

- **Power Management.** Enables power management.
- **Bootstrap Threshold.** Number of heartbeat misses before an AP reboots.
- **VoIP CAC Disconnect Extra Call.** Enables disconnecting of calls that exceed the high capacity threshold.
- **RF Band.** RF band in which the AP should operate: g = 2.4 GHz, a=5GHz.

Configuring Radio Settings

You can fine-tune radio settings on a per-radio (802.11a or 802.11b/g) basis.

	**Note:** Selecting these options may affect roaming performance.

To configure radio settings that affect all APs in the network, navigate to the Configuration > Advanced > WLAN > Network > Radio page.

To configure radio settings for APs in a specific location in the network:

1. Navigate to the Configuration > Advanced > WLAN > Advanced page.
2. Click Add to add a new location.
3. Enter a location ID in the format *building.floor.plan*, where each value is an integer.
4. Click Add.
5. Select the 802.11b/g or 802.11a tab to configure radio settings (Figure 5-5).

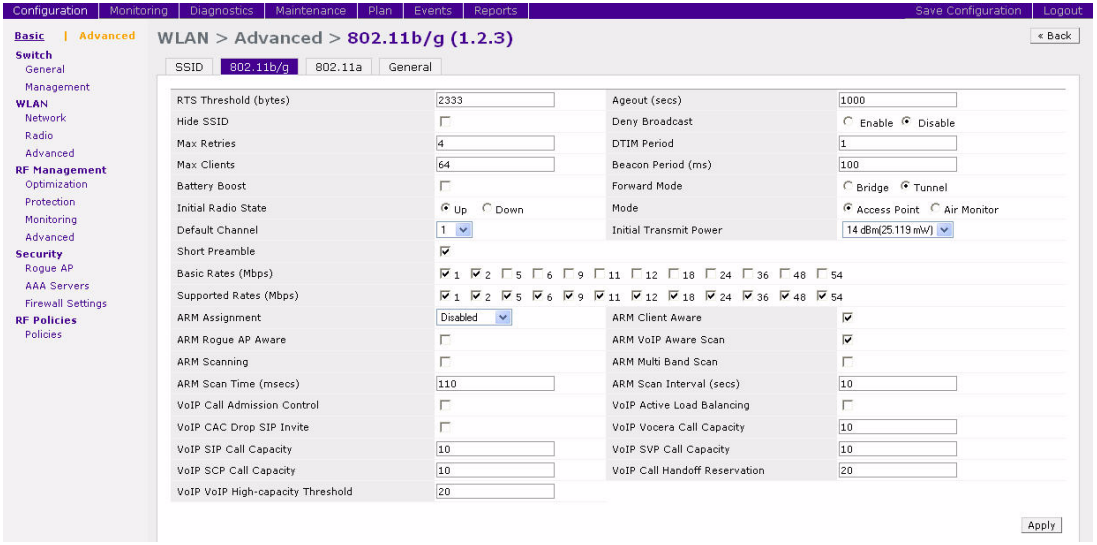

Figure 5-5

The radio configuration in the Advanced WLAN pages allow you to configure the following settings:

- **RTS Threshold.** Wireless clients transmitting frames larger than this threshold must issue Request to Send (RTS) and wait for the AP to respond with Clear to Send (CTS). This helps prevent mid-air collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting. The default is 2333 bytes.
- **Ageout.** Specifies the amount of time, in seconds, that a client is allowed to remain idle before being aged out. The default is 1000 seconds.
- **Hide SSID.** Enables or disables hiding of the SSID name in beacon frames.
- **Deny Broadcast.** When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients must know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.
- **Max Retries.** Specifies the maximum number of retries allowed for the AP to send a frame. The recommended range is between 3 and 7. The default is 3.

- **DTIM Period.** Specifies the interval between the sending of Delivery Traffic Indication Messages (DTIMs) in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed. When using wireless clients that employ power management features to sleep, the client must revive at least once during the DTIM period to receive broadcasts. The default is 2.
- **Max Clients.** Specifies the maximum number of wireless clients for a radio on an AP. The default is 0, but is set to 64 if the initial setup dialog is used to configure the WFS709TP.
- **Beacon Period.** Specifies the time between successive beacons being transmitted. The default is 100 milliseconds.
- **Battery Boost.** Converts multicast traffic to unicast before delivery to the client, thus allowing you to set a longer DTIM interval. The longer interval keeps associated wireless clients from activating their radios for multicast indication and delivery, leaving them in power-save mode longer and thus lengthening battery life.
- **Forward Mode.** Controls whether 802.11 frames are tunneled to the WFS709TP using generic routing encapsulation (GRE), or bridged into the local Ethernet LAN.
- **Initial Radio State**. Used to enable or disable the radio. Select Up to ensure that the AP radio is up on reboot.
- **Mode**. Specifies whether the AP should act as an access point or an air monitor.
- **Default Channel.** Specifies the default channel on which the AP operates, unless a better choice is available through either calibration or from RF Plan.
- **Initial Transmit Power.** Sets the initial transmit power on which the AP operates, unless a better choice is available through either calibration or from RF Plan.
- **Short Preamble.** Enables or disables short preamble for 802.11b/g radios. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using short preamble. To use only long preamble, disable short preamble. Legacy client devices that use only long preamble generally can be updated to support short preamble. The default is enabled.
- **Basic Rates.** Specifies the list of supported rates that are advertised in beacon frames and probe responses.
- **Supported Rates.** Specifies the set of rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error/loss rate of the client.

The radio configuration in the Advanced WLAN pages also allow you to configure IntelliFi RF Management (IRM) parameters, which are described in "IntelliFi RF Management" on page 5-19 and voice parameters, which are described in Chapter 14, "Configuring WFS709TP for Voice".

Example Configuration

The following example includes:

- An 802.11 a/b/g SSID called Corpnet with dynamic WEP.
- An 802.11 b/g SSID called Voice with static WEP.
- The AP in location 4.2.6 is set to have a guest SSID in addition to the other two SSIDs. The guest SSID is open.

To configure this system:

1. Configure the 802.11 a/b/g SSID Corpnet in the global location 0.0.0 with dynamic WEP (Figure 5-6).

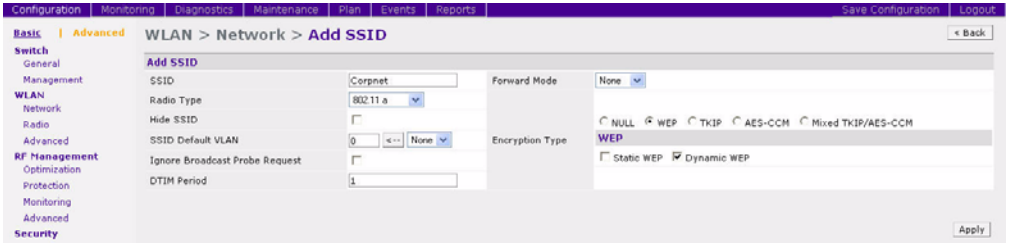

Figure 5-6

2. Configure the 802.11 b/g Voice SSID in the global location 0.0.0 with static WEP (Figure 5-7).

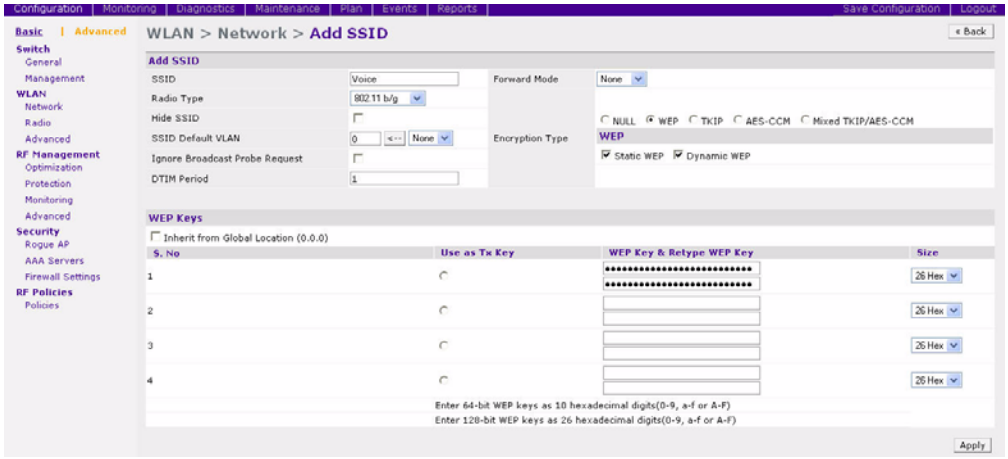

Figure 5-7

3. Configure the Guest SSID for location 4.2.6 (Figure 5-8).

Add the location 4.2.6.

Once the location is added, the location page is opened up with the inherited SSID. Click Add to add a new SSID Guest.

Configure the SSID with open system and native VLAN.

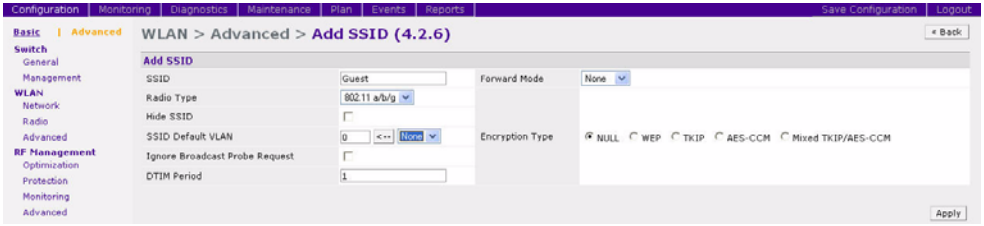

Figure 5-8

IntelliFi RF Management

IntelliFi RF Management (IRM) is an RF management technology for a stable, self-healing RF design. IRM takes the distributed algorithm approach, allowing APs to determine their transmit power and channel settings based on what they detect. The APs make their channel and power setting decisions based on the RF environment as they hear it, independent of the WFS709TP. This results in a highly scalable and reliable RF environment, while also significantly reducing the time the AP takes to adapt to changes in the RF environment.

The APs scan all valid channels in the regulatory domain at regular intervals and compute the following metrics per channel:

- *Coverage index*: Signal-to-noise ratio for all valid APs
- *Interference index:* Signal-to-noise ratio for all APs

These metrics are used by the APs and AMs to determine the channel and transmit power settings for optimal coverage.

Channel Setting

In addition to the interference index, the APs use the *free-channel index* to determine the optimal channel setting. The free-channel index is a configurable parameter on the WFS709TP used by an AP to qualify a channel before moving to it. An AP chooses to move to a new channel only if its current channel interference index is greater than the interference index on the new channel by a value greater than or equal to the free-channel index. If this requirement is not met, the AP remains on the current channel.

Power Setting

Power assignment decisions are based on the AP's coverage index. The benchmark used here is the *ideal-coverage* index. The ideal-coverage index is the power setting that an AP should have for good coverage. It is a configurable parameter on the WFS709TP. The AP increases or decreases its power settings based on the difference between the value of its current channel coverage index and the ideal-coverage index value. The power settings increment or decrement by a single unit at any given time.

Advantages of Using IRM

Using IRM provides the following benefits:

- The WFS709TP does not require a downtime for initial calibration.

- The AP response time to noise is quick and reliable, even to non-802.11 noise, especially when client traffic starts generating errors due to the noise.
- Non-802.11 noise detection is disabled by default and must be explicitly enabled.
- The IRM algorithm is based on what the AP hears, which means that the system can compensate for scenarios like broken antennas or blocked signal coverage on neighboring APs.
- Since channel decisions are based on the information the AP receives from the RF environment, interference due to third-party APs is taken into account.

Configuring IRM

1. Enable IRM for each AP and for the 802.11b/g radio.

- To enable IRM under the global setting, navigate to Configuration > Advanced > WLAN > Radio.
- To enable IRM for individual APs, navigate to Configuration > Advanced > WLAN > Advanced.
- To enable IRM on the 802.11b/g radio, navigate to the Configuration > Advanced > WLAN > Radio page (Figure 5-9).

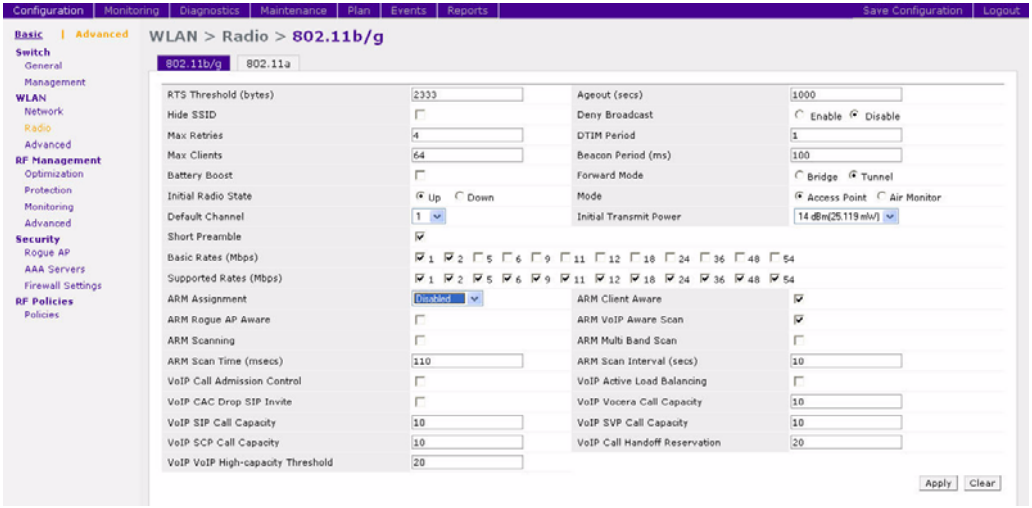

Figure 5-9

2. Set IRM Assignment to Single Band from the pull-down menu.

Note: The Multi Band option is currently unavailable. Selecting Multi Band automatically sets the selection to Single Band

3. Select IRM Scanning to enable scanning on the AP.
4. (Optional) Set the IRM Scan Interval and IRM Scan Time on a per-AP basis

   These values can be left to the default setting unless they need to be modified for a specific environment.
5. The AP scans the network and hops to the best available channel based on the IRM algorithm. Sometimes clients may not be able to adapt to this kind of dynamic AP channel change. To disable an AP from changing channels when an active client is connected to it, select IRM Client Aware.
6. Click Apply to apply the configurations.

Chapter 6
Configuring AAA Servers

You can use an external authentication server or an internal user database to authenticate users who need to access the wireless network.

This chapter describes how to configure theWFS709TP ProSafe Smart Wireless Switch to interface with an external Remote Authentication Dial-In User Service (RADIUS) server, and how to add entries into the internal database.

Note: In order for an external authentication server to process requests from the WFS709TP, you must configure the server to recognize the WFS709TP. Refer to the vendor documentation for the external authentication server for information on how to do this.

This chapter describes the following topics:

Configuring an External RADIUS Server

To configure RADIUS authentication servers on the WFS709TP:

1. Collect the following required information for RADIUS server configuration (Table 6-1).

Table 6-1. RADIUS Server Configuration Information

Parameter	Description
Server Name	Name of the RADIUS authentication server
IP Address	IP address of the authentication serve
Shared Secret	Shared secret between the WFS709TP and the authentication server
Authentication Port	Authentication port on the server (default is 1812)
Accounting Port	Accounting port on the server (default is 1813)

Table 6-1. RADIUS Server Configuration Information

Parameter	Description
Num Retries	Maximum number of retries sent to the server by the WFS709TP before the server is marked as down (default is 3)
Timeout	Maximum time, in seconds, that the WFS709TP waits before timing out the request and resending it (default is 5 seconds
NAS Source IP Address	Network Access Server (NAS) IP address to send in RADIUS packets.
NAS Identifier	NAS identifier to use in RADIUS packets.
Match ESSID	Match the ESSID for the user name
Match FQDN	Match the fully qualified domain name (FQDN) in the user name
Trim FQDN	Trim the FQDN from the user name before sending to the RADIUS server
Mode	Enables or disables the server

2. Navigate to the Configuration > Advanced > Security > AAA Servers > RADIUS Servers page.
3. Click Add to add a new RADIUS server entry. Enter the values you gathered into the fields shown in Figure 6-1.

Figure 6-1

4. Set the Mode to Enable to activate the authentication server.

> **Note:** When you configure a server, you can set the VLAN for users based on attributes returned for the user during authentication. These values take precedence over the default VLAN configured for the user. See "Configuring Authentication Timers" on page 6-4 for more information.

5. Click Apply to apply the configuration.

To edit or delete a RADIUS Server entry, click Edit or Delete in the Action column of the RADIUS server entry.

- If you are editing the entry, enter your changes, then click Apply to save the configuration.
- If you are deleting the entry, a pop-up window displays the message "Are you sure you want to delete the RADIUS server <server_name>?" Click OK to delete the entry.

Adding Users to the Internal Database

You can create entries in an internal database that can be used to authenticate users. The internal database contains a list of users along with the password for each user. When you configure the WFS709TP as the primary server, user information in incoming authentication requests is checked against the internal database.

To add a user to the internal database:

1. Collect the following information required for internal database entries (Table 6-2).

Table 6-2. Internal Database Entry Information

Parameter	Description
User Name	User name (mandatory field)
Password	Password (mandatory field)
E-mail	E-mail address of the user
Entry does not expire/ Expiration	No expiration on user entry, expiration duration (in minutes), or specific time and date of expiration. If an expiration is configured for the user, the user is disconnected at the expiration of the account. To continue network access, a user will need to authenticate using an unexpired account.

2. Navigate to the Configuration > Advanced > Security > AAA Servers > Internal Database page.
3. Click Add User in the Users section. The user configuration page displays.
4. Enter the information for the user.
5. Click Enabled to activate this entry on creation.
6. Click Apply to apply the configuration.

To edit or delete an internal database entry, click Edit or Delete in the Action column of the entry.

- If you are editing the entry, enter your changes, then click Apply to save the configuration.
- If you are deleting the entry, a pop-up window displays the message “Are you sure you want to delete user <user_name>?” Click OK to delete the entry.

Configuring Authentication Timers

You can configure the following timers that apply to all users and RADIUS servers:

- **User Idle Timeout**. The time, in minutes, that a client has to respond to the WFS709TP before it has to re-authenticate itself to gain access to the network. To prevent users from timing out, set the value in the field to 0.
- **Authentication Server Dead Time**. The maximum period, in minutes, that the WFS709TP considers an unresponsive authentication server to be down. This timer only applies when two or more authentication servers are configured on the WFS709TP. If there is only one authentication server configured, the server is never considered down and all requests are sent to the server.

  If one or more backup servers are configured and a server is unresponsive, it is marked as down for the dead time; subsequent requests are sent to the next server on the priority list for the duration of the dead time. If the server is responsive after the dead time has elapsed, it can take over servicing requests from a lower-priority server; if the server continues to be unresponsive, it is marked as down for the dead time.
- **Logon User Lifetime**

These timers can be left at the default values for most implementations.

To set an authentication timer:

1. Navigate to the Configuration > Advanced > Security > AAA Servers page; click the General tab if it is not already selected.

2. Configure the timers as described above.
3. Click Apply before moving on to another page or closing the browser window. Failure to do this results in loss of configuration, and you will have to reconfigure the settings.

.

Chapter 7
Configuring 802.1x Authentication

802.1x is an Institute of Electrical and Electronics Engineers (IEEE) standard that provides an authentication framework for wireless LANs (WLANs). 802.1x uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1x framework that are suitable for wireless networks include EAP-Transport Layer Security (EAP-TLS), Protected EAP (PEAP), and EAP-Tunneled TLS (EAP-TTLS). These protocols allow the network to authenticate the client while also allowing the client to authenticate the network.

This chapter describes the following topics:

802.1x Authentication

802.1x authentication consists of three components:

- The *supplicant*, or client, is the device attempting to gain access to the network. You can configure your system to support 802.1x authentication for wired users as well as wireless users.
- The *authenticator* is the gatekeeper to the network and permits or denies access to the supplicants. The WFS709TP ProSafe Smart Wireless Switch acts as the authenticator, relaying information between the authentication server and supplicant. The EAP type must be consistent between the authentication server and supplicant and is transparent to the WFS709TP.
- The *authentication server* provides a database of information required for authentication and informs the authenticator to deny or permit access to the supplicant.

  The 802.1x authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS) server that can authenticate either users (through passwords or certificates) or the client computer.

You can terminate the 802.1x authentication on the WFS709TP. The switch passes user authentication to its internal database or to a “backend” non-802.1x server. This feature, also called AAA FastConnect, is useful for deployments where an 802.1x EAP-compliant RADIUS server is not available or required for authentication.

Authentication with a RADIUS Server

Figure 7-1 is an overview of the parameters that you need to configure on authentication components when the authentication server is an 802.1x EAP-compliant RADIUS server.

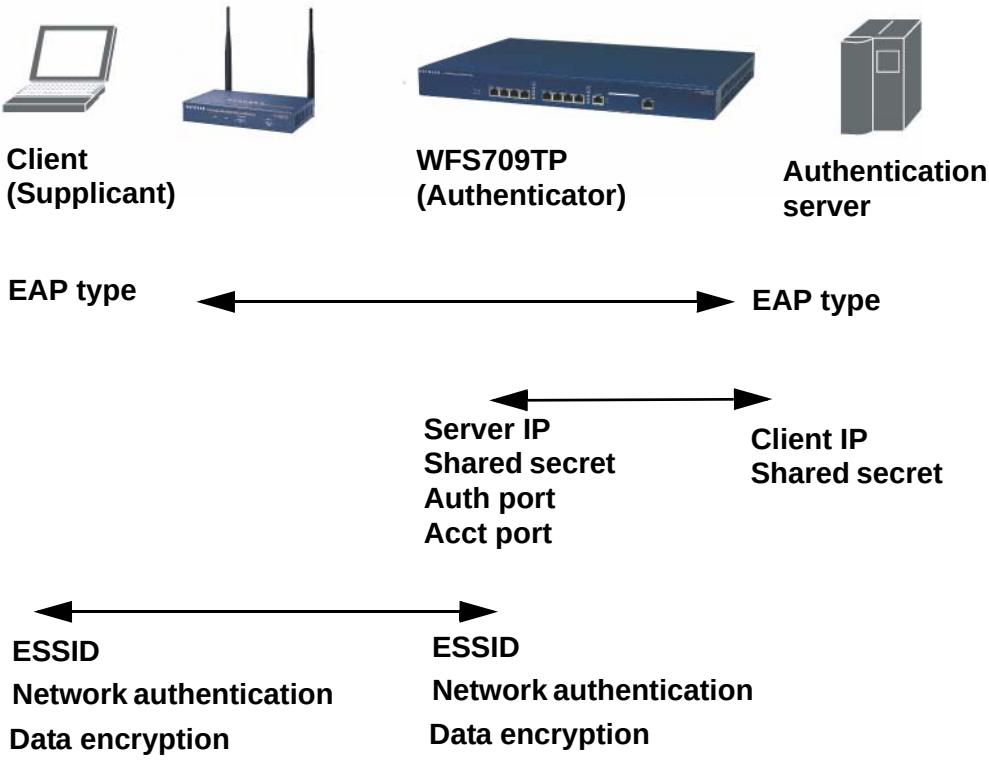

Figure 7-1

The supplicant and authentication server must be configured to use the same EAP type. The WFS709TP does not need to know the EAP type used between the supplicant and authentication server.

For the WFS709TP to communicate with the authentication server, you must configure the IP address, authentication port, and accounting port of the server on the WFS709TP. The authentication server must be configured with the IP address of the RADIUS client, which here is the WFS709TP. Both the WFS709TP and the authentication server must be configured to use the same shared secret.

As described in Chapter 1, "Overview of the WFS709TP", the client communicates with the WFS709TP through a Generic Routing Encapsulation (GRE) tunnel in order to form an association with an AP and to authenticate to the network. Therefore, the network authentication and encryption configured for an ESSID must be the same on both the client and the WFS709TP.

"Configuring 802.1x Authentication" on page 7-4 describes 802.1x configuration on the WFS709TP.

Authentication Terminated on WFS709TP

Figure 7-2 is an overview of the parameters that you need to configure on 802.1x authentication components when 802.1x authentication is terminated on the WFS709TP (AAA FastConnect). User authentication is performed either via the WFS709TP's internal database or by a non-802.1x server.

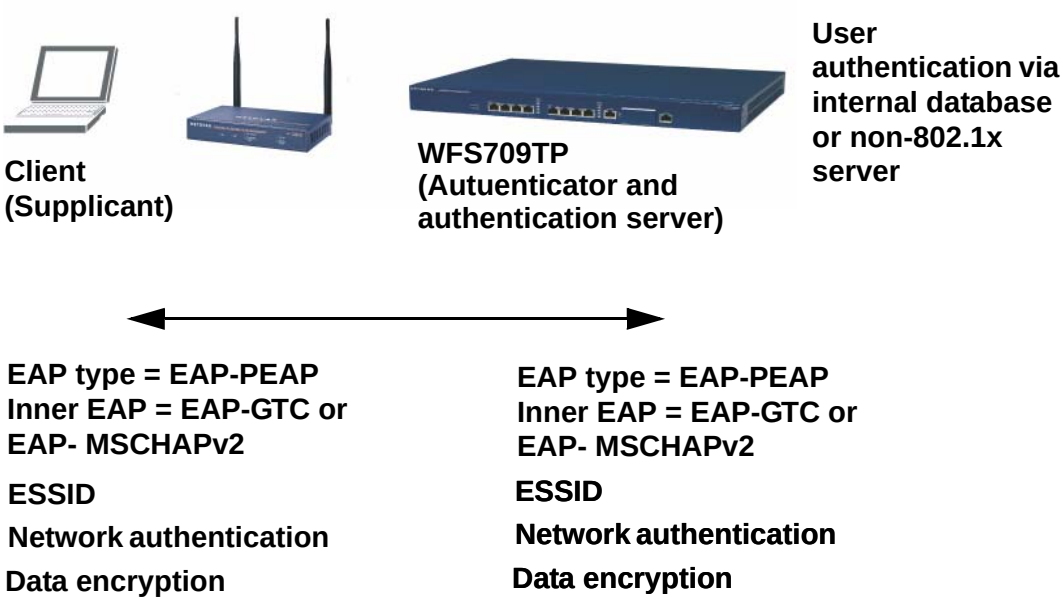

Figure 7-2

In this scenario, the supplicant must be configured for Protected EAP (PEAP), as the WFS709TP only supports PEAP. PEAP uses Transport Layer Security (TLS) to create an encrypted tunnel. Within the tunnel, one of the following EAP methods is used:

- EAP-Generic Token Card (GTC): Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of an LDAP or RADIUS server as the user authentication server. You can also enable caching of user credentials on the WFS709TP as a backup to an external authentication server.
- EAP-Microsoft Challenge Authentication Protocol version 2 (MS-CHAPv2): Described in RFC 2759, this EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the backend authentication server.

Note: You must install a server certificate in the WFS709TP for AAA FastConnect, as described in "Installing a Server Certificate" on page 13-19.

If you are using the WFS709TP's internal database for user authentication, you need to add the names and passwords of the users to be authenticated. If you are using an LDAP server for user authentication, you need to configure the LDAP server on the WFS709TP, and configure user IDs and passwords. If you are using a RADIUS server for user authentication, you need to configure the RADIUS server on the WFS709TP.

Configuring 802.1x Authentication

On the WFS709TP, use the following steps to configure a wireless network that uses 802.1x authentication:

1. Configure the 802.1x RADIUS authentication server.

Note: If you are using EAP-GTC within a PEAP tunnel, you can configure either an LDAP or a RADIUS server as the authentication server. If you are using AAA FastConnect, you can use a non-802.1x server or the WFS709TP's internal database. See Chapter 6, "Configuring AAA Servers".

2. Configure 802.1x authentication. See "802.1x Authentication Page" on page 7-5.
3. Configure the VLANs to which the authenticated users will be assigned. See Chapter 3, "Configuring Network Parameters".

4. Configure the WLAN, specifying the authentication and encryption that matches the wireless client configuration.

802.1x Authentication Page

In the browser interface, you configure 802.1x authentication in the Configuration > Advanced > Security > Authentication Methods > 802.1x Authentication page (Figure 7-3).

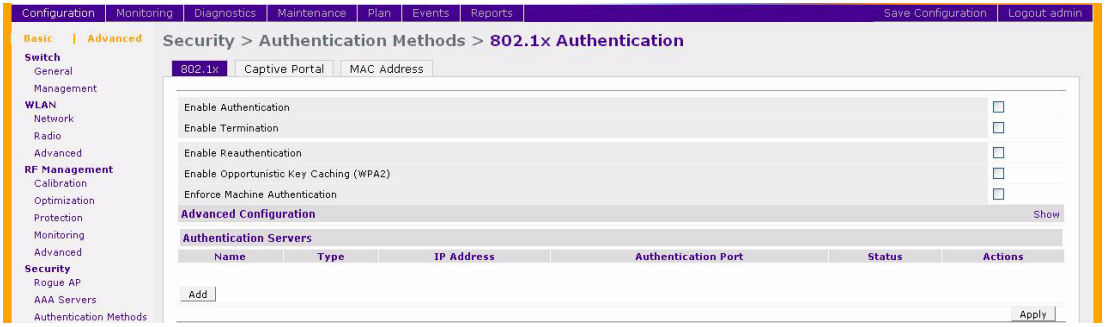

Figure 7-3

Table 7-1 describes the options on the 802.1x Authentication page:

Table 7-1. 802.1x Authentication Browser Interface Page Options

Parameter	Description	Default
Enable Authentication	Enable 802.1x authentication.	Disabled
Enable Termination	Terminate 802.1x authentication on the WFS709TP	Disabled
Enable Reauthentication	Select this option to force the client to do a 802.1x re-authentication after the expiration of the default timer for re-authentication. The default value of the timer is 24 hours (see “Advanced Configuration Options for 802.1x” on page 7-6). If the user fails to re-authenticate with valid credentials, the state of the user is cleared.	Disabled

Table 7-1. 802.1x Authentication Browser Interface Page Options (continued)

Parameter	Description	Default
Enable Opportunistic Key Caching (WPA2)	Enables the same pairwise master key (PMK) derived with a client and an associated AP to be used when the client roams to a new AP. This allows users faster roaming without having to reauthenticate. Make sure that the wireless client (the 802.1x supplicant) supports this feature before you enable this option. If the client does not support this feature, the client will attempt to renegotiate the key whenever it roams to a new AP. As a result, the key cached on the WFS709TP can be out of sync with the key used by the client.	Disabled
Enforce Machine Authentication *	Select this option to enforce machine authentication before user authentication.	Disabled

* For Windows environments only

Advanced Configuration Options for 802.1x

This section describes the Advanced Configuration options for 802.1x authentication (Figure 7-4). The Advanced Configuration settings should not be modified unless there is a need to customize at a more detailed level.

In the browser interface, access the Advanced options by clicking the Show tab on the right of the Advanced Configuration option on the 802.1x configuration page.

Figure 7-4

Table 7-2 describes the Advanced Configuration page fields.

Table 7-2. Advanced Authentication Fields

Field	Description	Default
Authentication Server Timeout	Time in seconds after which the authentication server is timed if it fails to respond.	30
Client Response Timeout	Time in seconds after which the client is timed out if it fails to respond.	30
Authentication Failure Timeout	Time in seconds after which the transaction is marked as failed if an authentication packet has not been received.	30
Client Retry Count	Number of attempts the WFS709TP makes to obtain an authentication from a client.	3
Server Retry Count	Number of attempts the WFS709TP makes to obtain an authentication from a server.	2
Key Retry Count	Number of attempts the WFS709TP makes to obtain the key.	1
Reauthentication Time Interval	The time period between re-authentication of supplicants. Unicast keys are updated after each re-authorization.	86400 seconds
Enable Multicast Key Rotation	Enables the rotation of multicast keys. Multicast keys are used to encrypt multicast packets generated for each AP. Multicast keys are associated with each SSID.	Disabled

Table 7-2. Advanced Authentication Fields (continued)

Field	Description	Default
Multicast Key Rotation Time Interval	The time period between each multicast key rotation.	1800 seconds
Enable Unicast Key Rotation	Enables the rotation of unicast keys. (Many wireless clients do not support this function.)	Disabled
Unicast Key Rotation Time Interval	The time period between each unicast key rotation.	900 seconds
Reset 802.1x Parameter to Factory Defaults	Resets the dot.1x settings to the factory defaults.	
Machine Authentication Cache Timeout	Sets the cache timeout for machine authentication.	24 hours
WPA Key Retry Count	The number of attempts the WFS709TP makes to obtain the WPA key.	3
WPA Key Timeout	Time in seconds after which the authentication server is timed out if the WPA key has failed to respond.	500
WPA Fast Handover	Enables fast handover for phones that support WPA and fast handover.	Disabled

.

Chapter 8
Configuring the Captive Portal

One of the methods of authentication supported by the WFS709TP ProSafe Smart Wireless Switch is Captive Portal. A Captive Portal presents a web page that requires action on the part of the wireless user before network access is granted. The required action can be simply viewing and agreeing to an acceptable use policy, or entering a user ID and password that must be validated against a database of authorized users.

This chapter describes the following topics:

Overview of Captive Portal Functions

There are two forms of Captive Portal you can configure for the WFS709TP.

- *Registration Web Page* requires no authentication; users typically enter an email address as an identification.
- *Captive Portal* requires users to be authenticated to an external authentication server or to the internal database on the WFS709TP.

	**Note:** While you can use Captive Portal to authenticate users, it does not provide for encryption of user data and should not be used in networks where data security is required. Captive Portal is most often used for guest access, access to open systems (such as public hot spots), or as a way to connect to a VPN.

You can use one or both forms of Captive Portal at the same time. The default Captive Portal web page provided with the WFS709TP displays login prompts for both registered users and guests. (You can customize the default Captive Portal page, as described in "Personalizing the Captive Portal Page" on page 8-6.)

If an appropriate server certificate is not installed in the WFS709TP, wireless clients that use Captive Portal may see a Security Alert message when logging in (Figure 8-1).

Figure 8-1

To prevent this message from appearing on clients, install a valid server certificate as described in "Installing a Server Certificate" on page 13-19.

You enable Captive Portal on a per-ESSID basis. Captive Portal users are initially allowed only DNS, DHCP, and HTTP or HTTPS connections to the network. Upon authentication, Captive Portal users are allowed full access to their assigned VLAN.

Note: MAC-based authentication, if enabled on the WFS709TP, takes precedence over Captive Portal authentication. If you use Captive Portal, do not enable MAC-based authentication.

Configuring Captive Portal

The following are the basic tasks for configuring Captive Portal in the base operating system:

- Configure the Captive Portal for guest or authenticated users. In the base operating system, you enable Captive Portal on a per-ESSID basis.
- If you are using Captive Portal to authenticate users, configure the authentication server that will be used to validate users. The authentication server can be either an external server or the WFS709TP's internal database.

The easiest way to complete these tasks is by using the browser interface Basic WLAN configuration page. Navigating to the Configuration > Basic > WLAN page allows you to configure an ESSID for either Registration Web Page or Captive Portal users.

To configure either Registration Web Page or Captive Portal for a single ESSID:

1. Navigate to the Configuration > Basic > WLAN page.
2. Enter the SSID name, for example WLAN-01.
3. Under 802.11 Security, select either Registration Web Page (for unauthenticated users) or Captive Portal (for authenticated users).

   If you select Captive Portal, you need to specify the authentication server that will validate the username and password for Captive Portal users:

   a. Click Add under Authentication Servers.
   b. Under Choose an Authentication Server, select the authentication server that will be the primary server.
   c. Click Add for the selection to be applied.
   d. To add additional authentication servers as backup servers, repeat the steps above.

   The servers appear in the order of descending priority. The first entry is always the primary server. To change the order, use the up or down arrows to move an entry higher up or lower down in the list.
4. Specify the VLAN to which users will be assigned.
5. Click Apply.

You can optionally configure other Captive Portal parameters by navigating to the Configuration > Advanced > Security > Authentication Methods > Captive Portal Authentication page. For example, if a proxy server is used for HTTP or HTTPS access, you need to explicitly allow TCP traffic between Captive Portal users and the proxy server.

Configuring Advanced Captive Portal Options

You configure advanced Captive Portal options in the Configuration > Advanced > Security > Authentication Methods > Captive Portal > Authentication page (Figure 8-2).

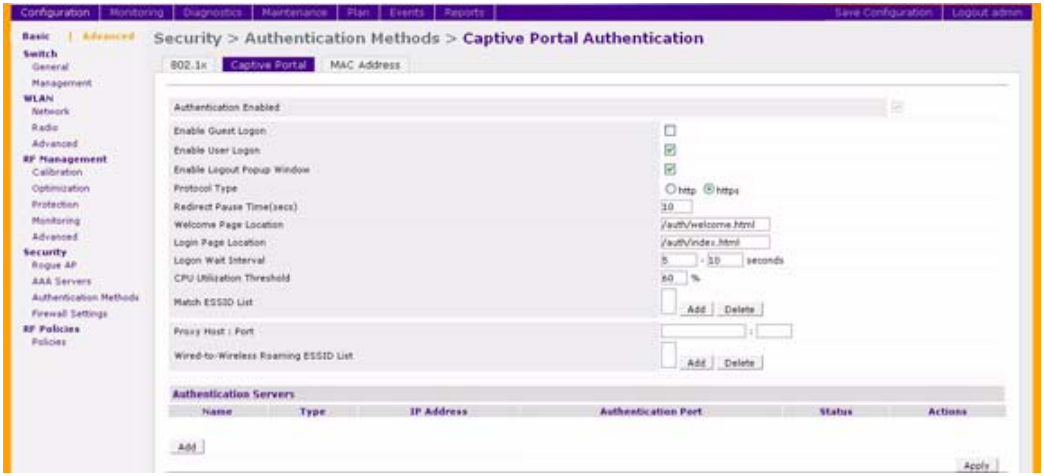

Figure 8-2

Table 8-1 describes the configuration options on this page.

Table 8-1. Captive Portal Authentication Browser Interface Page Options

Parameter	Description	Default
Authentication Enabled	Enables Captive Portal authentication.	
Enable Guest Logon	Enables Captive Portal logon without authentication.	Disabled
Enable User Logon	Enables Captive Portal with authentication of user credentials.	Enabled
Enable Logout Popup Window	When this option is enabled, a pop-up window appears with the Logout link for the user to log out. If this is disabled, the user remains logged in until the user timeout period or until the station reloads.	Enabled
Protocol Type	The protocol used on re-direction to the Captive Portal page. If you select HTTP, modify the captive portal policy to allow HTTP traffic.	https
Redirect Pause Time	The time, in seconds, that the system remains in the initial welcome page before re-directing the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link.	10
Welcome Page Location	The page that appears soon after logon and before re-direction to the web URL. This can be set to any URL.	/auth /welcome.html

Table 8-1. Captive Portal Authentication Browser Interface Page Options **(continued)**

Parameter	Description	Default
Login Page Location	The page that appears for the user logon. This can be set to any URL.	/auth /index.html
Logon Wait Interval	Time range, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. Works in conjunction with the CPU Utilization Threshold.	5–10 seconds
CPU Utilization Threshold	If CPU utilization is above this percentage, the Logon Wait Interval is applied.	60%
Match ESSID List (Base operating system only)	Specifies the ESSIDs on which the Captive Portal is enabled.	
Proxy Host: Port (Base operating system only)	Specifies the IP address of the proxy host and port used for HTTP or HTTPS access.	
Wired-to-Wireless Roaming ESSID List	Allows authenticated user to remain authenticated when roaming between wired and wireless networks.	

Select the options desired, then click Apply to apply the configuration.

Configuring the AAA Server for Captive Portal

The Captive Portal Authentication page allows you to choose the authentication servers to be used for user authentication:

1. From the Choose an Authentication Server a pull-down menu, to select the authentication server that will be the primary server.
2. Click Add for the selection to be applied.
3. To add additional authentication servers as backup servers, repeat steps 1 and 2.

   Servers are listed in order of descending priority. The first entry is always the primary server
4. (Optional) To change the list order, use the up or down arrows to move an entry higher or lower in the list.
5. Click Apply.

Changing the Protocol to HTTP

By default, HTTPS is used on redirection to the Captive Portal page. If you need to use HTTP instead, do the following:

1. Navigate to the Configuration > Advanced > Security > Authentication Methods > Captive Portal page.
2. For Protocol Type, select http and click Apply.

Personalizing the Captive Portal Page

You can personalize the following elements on the Captive Portal page:

- Captive Portal background
- Page text
- Acceptance Use Policy

To personalize the Captive Portal page:

1. Navigate to the Maintenance > Captive Portal > Customize Login page (Figure 8-3).

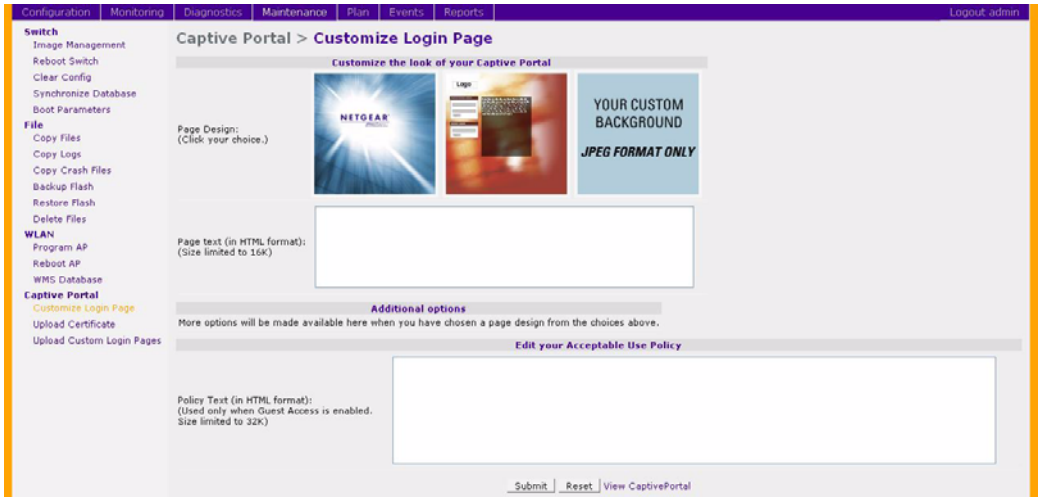

Figure 8-3

2. Select the page design.
   - Click an existing design to select it.
   - To customize the page background, select the YOUR CUSTOM BACKGROUND page. Under Additional options, enter the location of the JPEG image in the Upload... background field.

3. (Optional) Customize the captive portal background text.

   a. Set the background color in the Custom page background color field. The color code must a hexadecimal value in the format #hhhhhh.

   b. Click Submit on the bottom on the page.

   c. To view the background setting, click the View Captive Portal link. This displays the Captive Portal page as it will be seen by users (Figure 8-4).

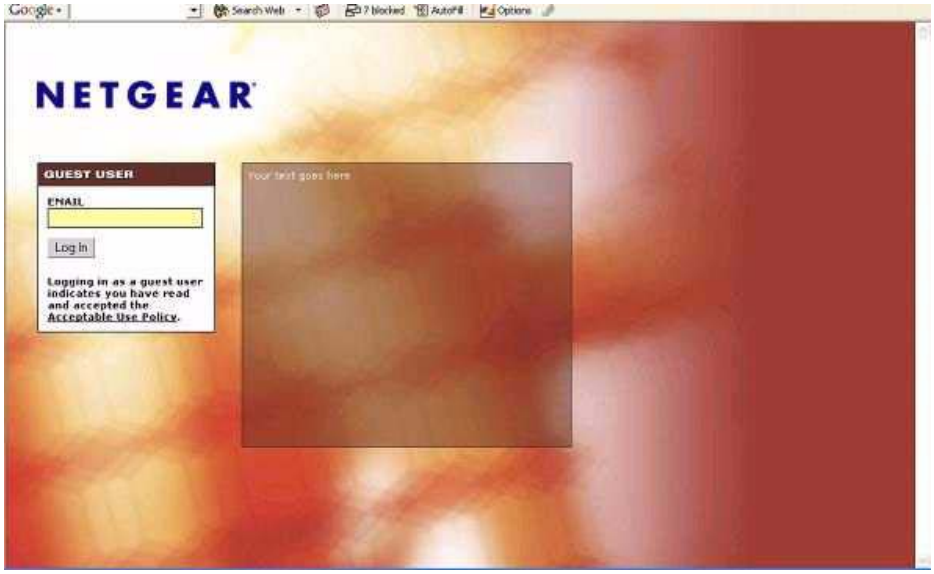

Figure 8-4

4. (Optional) Customize the captive portal background text:

   a. Enter the text that needs to be displayed (in HTML format) in the Page Text message box.

   b. To view the changes, click Submit at the bottom on the page and then click the View Captive Portal link. This displays the Captive Portal page as it will be seen by users.

5. (Optional) Customize the text under the Acceptable Use Policy:

   a. Enter the policy information in the Policy Text text box. This text appears only for a guest logon.

   b. To view the changes, click Submit at the bottom on the page and then click the View Captive Portal link. This displays the Captive Portal page as it will be seen by users (Figure 8-5).

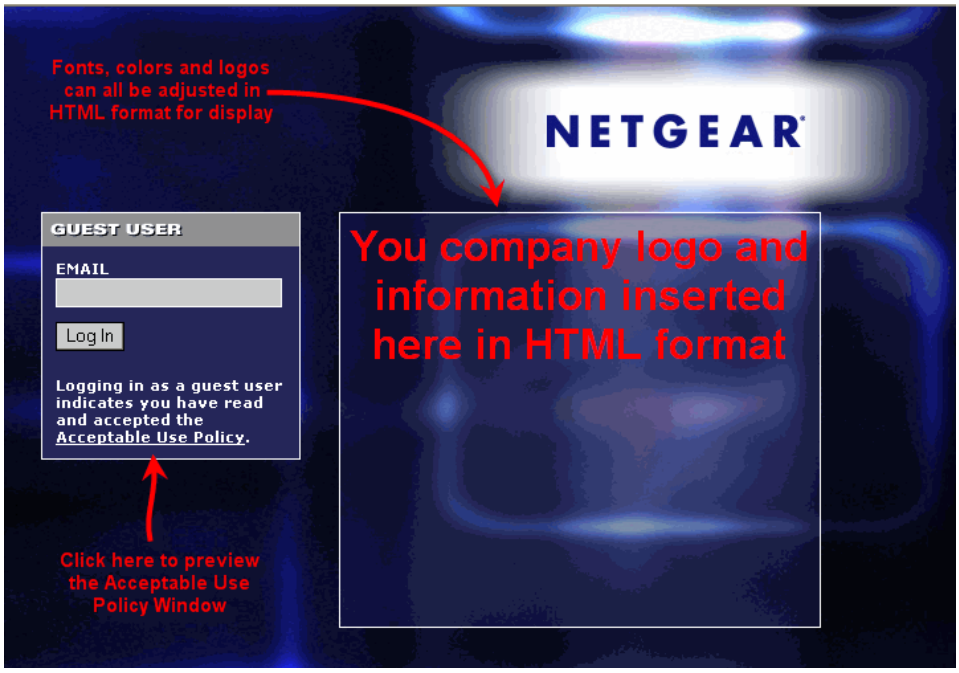

Figure 8-5

The text you entered appears in a text box when the user clicks the Acceptable Use Policy on the Captive Portal web page.

Chapter 9
Configuring MAC-Based Authentication

This chapter describes how to configure media access control (MAC) based authentication on the WFS709TP ProSafe Smart Wireless Switch using the browser interface.

Use MAC-based authentication to authenticate devices based on their physical MAC address. While not the most secure and scalable method, MAC-based authentication implicitly provides an additional layer of security to authentication devices. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to the rest. For example, if users are allowed access to the network via station A, then one method of authenticating station A is MAC-based. Users may be required to authenticate themselves using other methods depending on the network privileges required.

MAC-based authentication can also be used to authenticate W-Fi phones as an additional layer of security to prevent other devices from accessing the voice network using what is normally an insecure SSID.

This chapter contains the following topics:

Configuring the WFS709TP

Before configuring MAC-based authentication on the WFS709TP, you must first configure the authentication server that the WFS709TP uses to validate the users. The internal database can be used to configure the users for MAC-based authentication. See "Configuring Users" on page 9-2 for information on configuring the users on the local database. For information on configuring AAA servers, see Chapter 6, "Configuring AAA Servers".

To enable MAC-based authentication on the WFS709TP:

1. Navigate to the Configuration > Advanced > Security > Authentication Methods > MAC Address page (Figure 9-1).

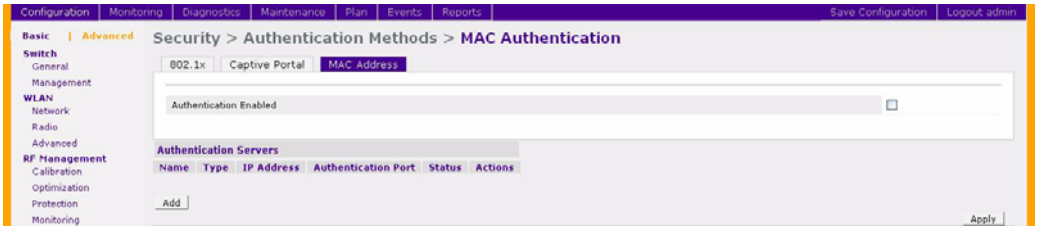

Figure 9-1

2. Check the Authentication Enabled checkbox to enable authentication.
3. Configure the authentication servers. This is the authentication server to which the WFS709TP will send authentication requests.

   a. To add an authentication server, click Add under Choose an Authentication Server.

	Note: Select the internal database option to use the local database on the WFS709TP for MAC-based authentication.

   b. From the pull-down menu, select the RADIUS server that will be the primary authentication server. Click Add after making the choice.

   c. To add multiple authentication servers, repeat steps a and b for each server.

   The servers appear in the order of descending priority. The first entry is always the primary server. To change the order, use the up or down arrows to move an entry higher up or lower down in the list.

4. Click Apply to apply and verify the changes made.

Configuring Users

This section explains how to configure users in the local database for MAC-based authentication:

To authenticate users using MAC-authentication by adding a user to the local database:

1. Navigate to the Configuration > Advanced > Security > AAA Servers > Internal Database page.
2. Under the Users section click Add User. This opens the Add User page (Figure 9-2).

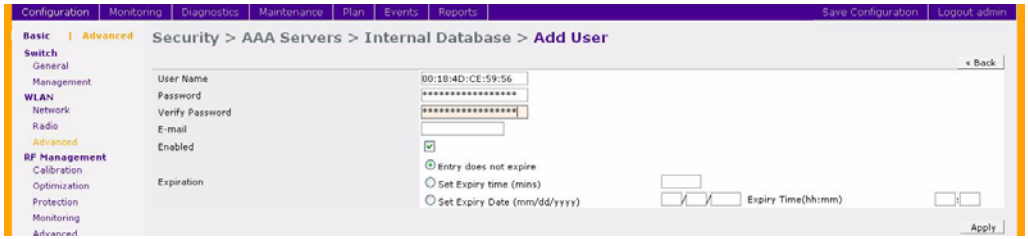

Figure 9-2

3. Enter the user information.

   a. In the User Name field, enter the MAC address of the device to be used, (this is the MAC-address of the physical interface that will be used to access the network). By default, the entry should be in the format xxxxxx.

   b. Enter the same address in the same format in the Password and Verify Password fields.

   c. Select the Enabled checkbox to activate the user.

4. Click Apply to apply the settings.

To delete a user from the database:

1. Navigate to the Security > AAA Servers > Internal Database page.
2. Click Delete to the right of the user you wish to delete.

To disable a user:

1. Navigate to the Security > AAA Servers > Internal Database page.
2. Click Disable to the right of the user you wish to disable.

   The user's entry will still exist in the database, but it will not be used for authentication purposes.

Chapter 10
Adding Local WFS709TPs

This chapter explains how to expand your network by adding a local WFS709TP ProSafe Smart Wireless Switch to a master WFS709TP configuration. Typically, this is the first expansion of a network with just one WFS709TP (which is a by definition a master switch). This chapter is a basic discussion of creating master-local WFS709TP configurations. More complicated multi-switch configurations are discussed Chapter 11, “Configuring Redundancy”.

This chapter describes the following topics:

Moving to a Multi-Switch Environment

For a single WLAN configuration, the master switch is the WFS709TP that controls the RF and security settings of the WLAN. Additional WFS709TPs to the same WLAN serve as local switches to the master WFS709TP. A local WFS709TP operates independently of the master WFS709TP and depends on the master WFS709TP only for its security and RF settings. You configure the Layer 2 and Layer 3 settings on the local WFS709TP independent of the master WFS709TP. The local WFS709TP needs to have connectivity to the master WFS709TP at all times to ensure that any changes on the master are propagated to the local WFS709TP.

Some of the common reasons to move from a single-switch to a multi-switch WFS709TP environment include:

- Scaling to include a larger coverage area
- Setting up remote access points (APs)
- Network setup requires APs to be redistributed from a single WFS709TP to multiple WFS709TPs

Configuring Local WFS709TPs

A single master WFS709TP configuration can be one WFS709TP or a *master redundant configuration* with one master WFS709TP and the VRRP redundant backup WFS709TP. This chapter covers migration to both of those scenarios.

The steps involved in migrating from a single-switch to a multi-switch WFS709TPenvironment are:

1. Configure the role of the local WFS709TP to local and specify the IP address of the master.
2. Configure the Layer 2 / Layer 3 settings on the local WFS709TP (VLANs, IP subnets, IP routes).
3. Configure as trusted ports the ports the master and local WFS709TP use to communicate with each other.
4. For those APs that need to boot off the local WFS709TP, configure the LMS IP address to point to the new local WFS709TP.
5. Reboot the APs that are already on the network, so that they now connect to the local WFS709TP.

Configuring the Local WFS709TP

To set the WFS709TP as local:

- Set the mode of the WFS709TP to local.
- Set the master IP address to the IP address of the master WFS709TP. If master redundancy is enabled on the master, this address should be the VRRP address for the VLAN instance corresponding to the IP address of the WFS709TP (see Figure 10-1).

Figure 10-1

Configuring L2/L3 Settings

- Configure the VLANs, subnets, and IP address on the local WFS709TP for IP connectivity.

- Verify connectivity to the master WFS709TP by pinging it from the local WFS709TP.
- Ensure that the master WFS709TP recognizes the new WFS709TP as its local WFS709TP.

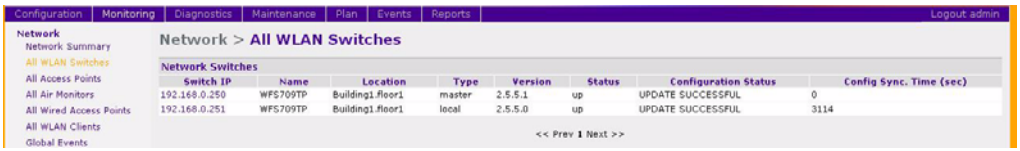

Figure 10-2

The local WFS709TP should be listed with type local in the Monitoring > Network > All WLAN Switches page on the master (see Figure 10-2). It takes about 4–5 minutes for the master and local WFS709TPs to synchronize configurations.

Configuring Trusted Ports

- On the local WFS709TP, navigate to the Configuration > Advanced > Switch > General > Port page and make sure that the port connecting to the master WFS709TP is trusted.
- On the master WFS709TP, make sure that the port connecting to the local WFS709TP is trusted.

Configuring APs

For APs that boot from the local WFS709TP, you must configure the LMS IP address under the AP's location ID. This configuration has to be done on the master WFS709TP. When the changes are applied, the master WFS709TP pushes these configurations to the local WFS709TP.

To configure the LMS IP address:

1. Navigate to the Configuration > Advanced > WLAN > Advanced > General page.
2. Configure the LMS IP (see Figure 10-3).

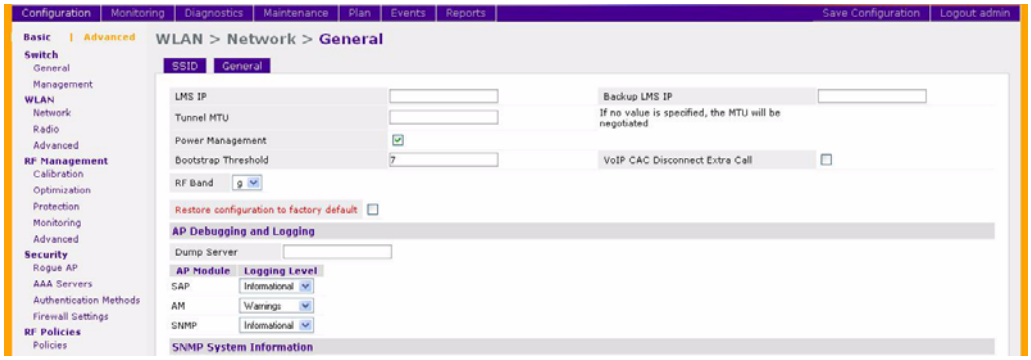

Figure 10-3

3. Apply the configuration on the master.

	Note: To verify that the local WFS709TP has obtained a copy of the global settings, check the local WFS709TP for the global configuration changes made on the master, such as authentication changes and WMS settings.

Rebooting APs

The configuration changes take effect only after rebooting the affected APs; this allows them to reassociate with the local WFS709TP. In the example shown in Figure 10-3, AP 1.1.20 will be rebooted. After rebooting, these APs appear to the new local WFS709TP as local APs (Figure 10-4).

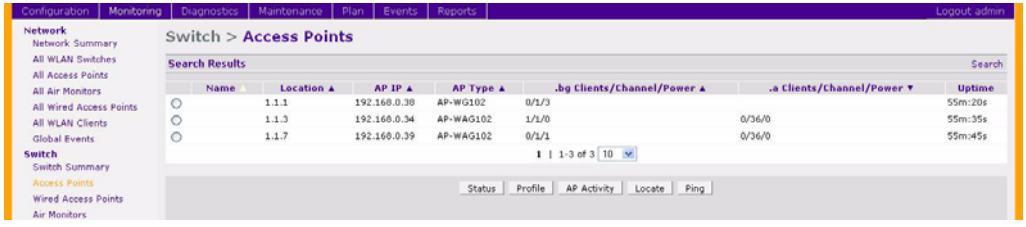

Figure 10-4

Chapter 11
Configuring Redundancy

This chapter describes the following topics:

Virtual Router Redundancy Protocol

The underlying mechanism for NETGEAR's redundancy solutions is the Virtual Router Redundancy Protocol (VRRP). This mechanism can be used to create various redundancy solutions, including the following:

- Pairs of local WFS709TP ProSafe Smart Wireless Switches acting in an active-active mode or a hot-standby mode
- A master WFS709TP backing up a set of local WFS709TPs
- A pair of WFS709TPs acting as a redundant pair of master WFS709TPs in a hot-standby mode

VRRP is designed to eliminate a single point of failure by providing an election mechanism for WFS709TPs to elect a "master" WFS709TP. This master WFS709TP is the owner of the configured Virtual IP (VIP) address for the VRRP instance. When the master becomes unavailable, one of the backup WFS709TPs takes the place of the master and owns the Virtual IP address. All network elements (such as the APs and other WFS709TP) can be configured to access the Virtual IP, thereby providing a transparent redundant solution to the rest of the network.

Redundancy Configuration

In a WFS709TP ProSafe Smart Wireless Switch system, all access points (APs) are controlled by a WFS709TP switch. The APs tunnel all data to the WFS709TP, which processes the data, including encryption/decryption, bridging/forwarding, and so on.

Local WFS709TP redundancy refers to providing redundancy for a WFS709TP such that the APs under its control failover to a backup WFS709TP if their master WFS709TPr becomes unavailable. Local WFS709TP redundancy is provided by running VRRP between a pair of WFS709TPs.

Note: The two WFS709TPs need to be connected on the same broadcast domain (or Layer 2 connected) for VRRP operation, and both should be running the same firmware version.

The APs are then configured to connect to the VIP configured for the VRRP instance.

Configuring Local WFS709TP Redundancy

To configure redundancy for a local WFS709TP:

1. Collect the following information needed to configure local WFS709TP redundancy:
   - VLAN ID on the two local WFS709TPs that are on the same Layer 2 network and will be used to configure VRRP
   - Virtual IP address to be used for the VRRP instance
2. Navigate to the Configuration > Advanced> Switch > General > VRRP page on the browser interface for each of the local WFS709TPs. Click Add to create a VRRP instance.

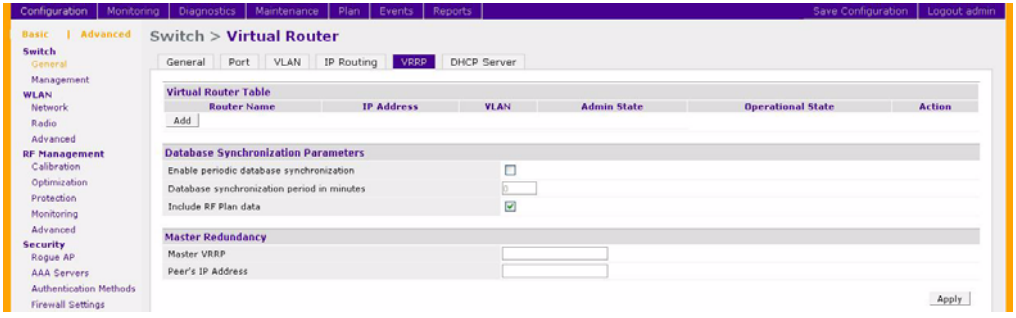

Figure 11-1

3. Enter the VRRP parameters for the VRRP instance.

   Table 11-1 explains what each of the parameters means and the recommended/expected values for this configuration.

Table 11-1. VRRP Parameters for Local WFS709TP Redundancy

Parameter	Explanation	Expected or Recommended Values
Virtual Router ID	The Virtual Router ID that uniquely identifies this VRRP instance.	Configure this with the same value as the VLAN ID for easy administration.
Recommended to Advertisement Interval	The interval between successive VRRP advertisements sent by the current master.	Recommended to leave as default (1000ms = 1s).
Authentication Password	An optional password that can be used to authenticate VRRP peers in their advertisements.	This is an optional password that can be used to authenticate VRRP peers in their advertisements.
Description	An optional textual description to describe the VRRP instance.	
IP Address	The Virtual IP address that will be owned by the elected VRRP master.	Configure this with the Virtual IP address.
Enable Router Pre-emption	A WFS709TP can take over the role of master if it detects a lower priority WFS709TP currently acting as master.	For this topology, it is recommended *not* to select this option.
Priority	Priority level of the VRRP instance for the WFS709TP. This value is used in the election mechanism for the master.	It is recommended to leave this as the default for this topology (default = 100).
Tracking	Configures a tracking mechanism that adds a specified value to the priority after a WFS709TP has been the master for the VRRP instance. This mechanism is used to avoid failing over to a backup Master for transient failures. Tracking can be based on one of the following: • Master Up Time: how long the switch has been the master. • VRRP Master State Priority: the master state of another VRRP.	Recommended to leave this as the default for this topology (default = 100).

Table 11-1. VRRP Parameters for Local WFS709TP Redundancy (continued)

Parameter	Explanation	Expected or Recommended Values
Admin State	Administrative state of the VRRP instance.	To start the VRRP instance, change the admin state to UP.
VLAN	VLAN on which the VRRP protocol will run.	Configure this to be the VLAN ID.

4. Configure the values in the respective fields and click Done to enter the values.
5. Click Apply to apply the configuration and add the VRRP instance.
6. Configure the APs to terminate their tunnels on the Virtual IP address. "Configuring APs" on page 10-3.

Note: This command must be executed on the master WFS709TP, as only the master WFS709TP controls all APs in the network.

Master WFS709TP Redundancy

The master WFS709TP acts as a single point of configuration for global policies such as authentication parameters and RF configuration to ease the configuration and maintenance of a wireless network. It also maintains a database related to the wireless network that is used to make both automated and manual adjustments in reaction to events that cause a change in the environment (such as an AP becoming unavailable). The master WFS709TP is also responsible for providing the configuration for any AP to complete its boot process. If the master becomes unavailable, the network continues to run without any interruption. However any change in the network topology or configuration will require the availability of the master WFS709TP.

To maintain a highly redundant network, the administrator can use another WFS709TP to act as a hot standby for the master WFS709TP. The underlying protocol used is also VRRP.

To configure master WFS709TP redundancy:

1. Collect the following data:
   - VLAN ID on the two WFS709TPs that are on the same layer 2 network and will be used to configure VRRP
   - Virtual IP address that has been reserved to be used for the VRRP instance
2. Navigate to the Configuration > Advanced> Switch > General > VRRP page on the browser interface for each of the master WFS709TPs. Click Add to create a VRRP instance.

3. Enter the parameters shown in Table 11-1. For this topology, the following values are recommended:
   - Priority: Set the “initially preferred” master to 110 and set the backup master to 100.
   - Enable pre-emption.
   - Configure master up time or master state tracking with an add value of 20.
4. Configure the values in the respective fields, then click Done to enter the values.
5. Click Apply to apply the configuration and add the VRRP instance.
6. Associate the VRRP instance with the master WFS709TP redundancy (see Table 11-2).

Table 11-2. VRRP Associations

Association	Function	Switch ID
Master VRRP	Associates a VRRP instance with master redundancy	Virtual Router ID of the VRRP instance
Peer’s IP Address	Loopback IP address of the peer for master redundancy	Loopback IP address of the peer WFS709TP

7. Configure the APs to terminate their tunnels on the Virtual IP address. See “Configuring APs” on page 10-3.

Note: All the APs and local WFS709TPs in the network should be configured with the VIP address as the master IP address.

The master IP address is configured for local WFS709TPs during the initial setup of the switch. You can also change the master IP address configured on the local WFS709TP in the Configuration > Advanced > Switch > General page in the browser interface.

The WFS709TP requires a reboot after you change the master IP of the WFS709TP.

If Domain Name Service (DNS) resolution is the chosen mechanism for the APs to discover their master WFS709TP, ensure that the name “netgear-master” resolves to the same VIP address configured as a part of the master redundancy.

Master-Local WFS709TP Redundancy

This section outlines the concepts behind a redundancy solution where a master can act as a backup for one or more local WFS709TPs, and shows how to configure the WFS709TPs for such a redundant solution. In this solution, the local WFS709TPs act as the switches for the APs. When

any one of the local WFS709TPs becomes unavailable, the master takes over the APs controlled by that local WFS709TP for the time that the local WFS709TP remains unavailable. When the local WFS709TP comes back again, it resumes control over the APs.

This type of redundant solution is illustrated by Figure 11-2.

Note: This solution requires that the master WFS709TP have Layer 2 connectivity to all the local WFS709TPs.

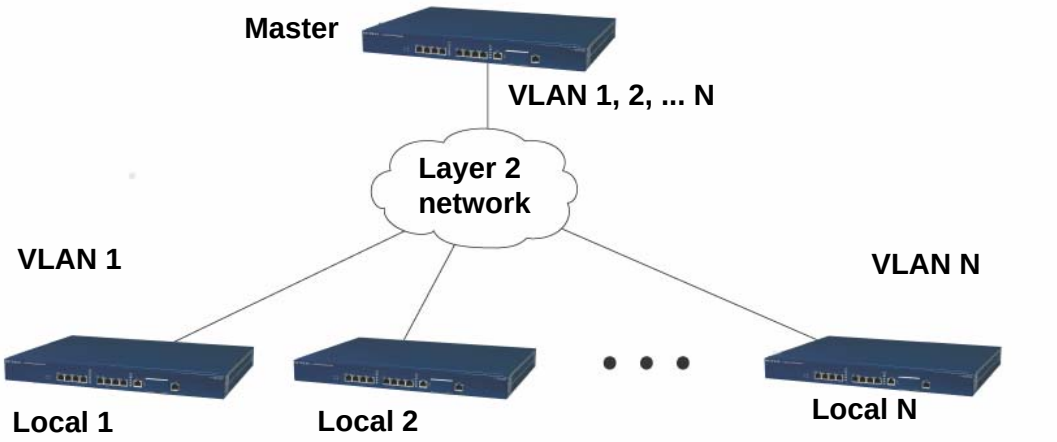

Figure 11-2

In the network shown in Figure 11-2, the master WFS709TP is connected to the local WFS709TPs on VLANs 1, 2… n respectively through a Layer 2 network. To configure redundancy, configure VRRP instances on each of the VLANs between the master and the respective local WFS709TP. The VRRP instance on the local WFS709TP is configured with a higher priority to ensure that when it is available, the APs always choose the local WFS709TP to terminate their tunnels.

To configure the master and local WFS709TPs for such a topology:

1. Configure the interface on the master WFS709TP to be a trunk port with 1, 2… n being member VLANs.
2. Collect the following data:
   - VLAN IDs on the WFS709TP corresponding to the VLANs 1, 2…n shown in the topology above

- Virtual IP addresses that have been reserved to be used for the VRRP instances

3. Navigate to the Configuration > Advanced> Switch > General > VRRP page.
4. Enter the parameters shown in Table 11-1. For this topology, the following values are recommended:
   - Priority: Set the master to 100 and set the local to 110
   - Enable pre-emption
   - Configure master up time or master state tracking on the master with an add value of 20
5. Configure the values in the respective fields and click Done to enter the values.
6. Click Apply to apply the configuration and add the VRRP instance.

Note: The master WFS709TP is configured with the number of VRRP instances equal to the number of local switches to which the master is providing redundancy.

Configure the APs with the appropriate Virtual-IP address depending on which WFS709TP is expected to control the AP. As an example, the administrator can configure all APs on floor 1 to be controlled by local WFS709TP 1, all APs on floor 2 to be controlled by local WFS709TP 2, and so on. All the local WFS709TPs are backed up by the master WFS709TP, as shown above. In such a case, configure all APs on floor 1 to be controlled by the Virtual IP address of the VRRP between local WFS709TP 1 and master, and so on. See “Configuring APs” on page 10-3.

.

Chapter 12
Configuring Wireless Intrusion Protection

This chapter outlines configuring various wireless intrusion protection features. The topics covered are:

Rogue/Interfering AP Detection

The most important intrusion protection functionality offered in the WFS709TP ProSafe Smart Wireless Switch system is the ability to classify an access point as either a rogue AP or an interfering AP. An AP is considered to be a *rogue AP* if it is both unauthorized and plugged into the wired side of the network. An AP is considered to be an *interfering AP* if it is seen in the RF environment but is not connected to the wired network. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat.

You can enable a policy to automatically disable APs that are classified as rogue APs by the system. When a rogue AP is disabled, no wireless stations are allowed to associate to that AP. Refer to "Configuring Rogue AP Detection" on page 12-4 for details on how to configure Rogue AP detection, classification, and containment.

You can manually reclassify an interfering AP. Refer to "Classifying APs" on page 12-2 for details on how to change the classification of an AP.

Enabling AP Learning

AP learning allows the system to classify all newly discovered APs as valid APs. By default, AP learning is not enabled and all newly discovered APs are classified as interfering APs. You can enable or disable AP learning from the browser interface.

	**Note:** Enabling AP learning is useful when you install the WFS709TP in an environment with an existing third-party wireless network, especially if there are a large number of installed APs. Leave AP learning enabled until all APs in the network have been detected and classified as valid. Then disable AP learning and reclassify any unknown APs as interfering.

To enable or disable AP learning:

1. Navigate to the Configuration > Advanced > Security > Rogue AP page on the master WFS709TP (Figure 12-1).

Figure 12-1

2. Enable or disable AP learning.
   - To enable AP learning, select the option “Mark All New Access Points as Valid Access Points”
   - To disable AP learning, deselect this option.
3. Click Apply.

Classifying APs

If AP learning is enabled, every newly discovered AP is classified as a valid AP. If AP learning is disabled, every newly discovered AP is classified as an interfering AP. You can also manually classify individual APs. For example, if you know about an interfering AP, you can manually reclassify it as a known interfering AP. You can manually classify an AP into one of the following categories:

- **Valid AP**. An AP that is part of the enterprise providing WLAN service. APs that successfully connect to the WFS709TP and load software and configuration should be classified as valid APs.

> **Note:** Any client that successfully authenticates with a valid AP and passes encrypted traffic is classified as a valid client. (Encrypted traffic includes encrypted 802.11 frames and unencrypted 802.11 frames that are VPN encrypted.)

- **Interfering AP or Known Interfering AP**. An AP that is seen in the RF environment but is not connected to the wired network. An interfering AP is not considered a direct security threat since it is not connected to the wired network.
- **Unsecure AP**. An rogue AP that is part of the network. A rogue AP is an unauthorized AP that is plugged into the wired side of the network.
- **DoS AP.** An AP on which denial of service is enabled.

To manually classify an AP:

Navigate to the Reports > AP Reports> All Interfering APs page on the master WFS709TP (Figure 12-2).

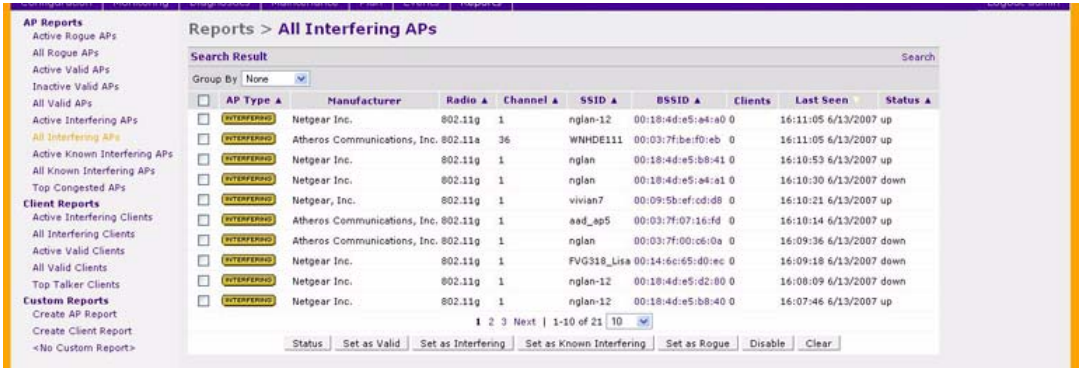

Figure 12-2

4. Select the checkboxes for the APs you want to classify.
5. Click the appropriate “Set as” button on the page.
6. Click Apply.

Configuring Rogue AP Detection

Follow the steps below to configure the network to detect insecure APs and to classify them as rogue and interfering respectively as defined in the section above.

Navigate to the Configuration > Advanced > Security > Rogue AP page on the browser interface of the master WFS709TP (Figure 12-3).

Figure 12-3

Table 12-1 explains the fields for this configuration and what it means to select each of them.

Table 12-1. AP Classifications

FIeld	Description
Disable Users from Connecting to Rogue Access Points	By default, rogue APs are only detected, but are not automatically disabled. Enable this option to automatically shut down rogue APs. When this option is enabled, clients attempting to associate to a rogue AP will be disconnected from the rogue AP through a denial of service attack.
Mark All New Access Points as Valid Access Points	When installing a WFS709TP in an environment with an existing third-party wireless network, it is necessary to manually classify existing enterprise APs as valid—a time-consuming process if a large number of APs are installed. Enable this option to mark all detected APs as valid. Leave this option enabled until all enterprise APs have been detected and classified as valid. After this process has completed, disable this option and re-classify any unknown APs as interfering.
Mark Unknown Access Points as Rogue Access Points	In an environment where no interfering APs should exist—for example, a building far away from any other buildings or an RF-shielded building—enable this option to turn off the classification process. Any AP detected that is not classified as valid will be marked as rogue.

Note: Use caution when enabling both “Mark Unknown APs as Rogue” and “Disable Users from Connecting to Rogue APs.” If the system is installed in an area where APs from neighboring locations can be detected, these two options will disable all APs in the area.

Misconfigured AP Detection

If desired, you can specify the valid channels for an AP. This capability is primarily used when third-party APs are being used in the network, since the WFS709TP cannot configure the third-party APs. If a valid AP is detected as misconfigured, the system will deny access to the misconfigured AP. In cases where someone gains configuration access to a third-party AP and changes the configuration, this policy is useful in blocking access to that AP until the configuration can be fixed.

Configuring Misconfigured AP Protection

An AP is classified as misconfigured if it does not meet configured valid channels. To configure protection for misconfigured APs, navigate to Configuration > Advanced > RF Policies > Policies > Misconfigured AP as shown in Figure 12-4.

Figure 12-4

Table 12-2 describes the fields shown in this section.

Table 12-2. Valid Channel Types

Field	Description
Valid Enterprise 802.11b/g Channels	Defines the list of valid 802.11b/g channels that third-party APs are allowed to use.
Valid Enterprise 802.11a Channels	Defines the list of valid 802.11a channels that third-party APs are allowed to use.

Chapter 13
Configuring Management Utilities

This chapter describes management utilities for a WFS709TP ProSafe Smart Wireless Switch wireless network.

This chapter includes the following topics:

Configuring Management Users

You can assign one of the following predefined user roles when configuring management users:

- **root:** permits access to all management functions on the WFS709TP
- **read-only:** permits access to browser interface monitoring pages only
- **guest-provisioning:** permits access to adding and configuring guest users in the WFS709TP's internal database only
- **network-operations:** permits access to Monitoring pages in the browser interface operations that are useful for monitoring the WFS709TP

To configure management users from the browser interface:

1. Navigate to the Configuration > Advanced > Switch > Management > Access Control page.
2. Under Management Users, click Add.
3. Enter the name and password for the user.
4. Select the predefined user role for the user.
5. Click Apply.

Configuring SNMP

WFS709TP switches and access points (APs) support versions 1, 2c, and 3 of SNMP for reporting purposes only. SNMP cannot be used for setting values in a WFS709TP system in the current version.

SNMP for the WFS709TP

Follow the steps below to configure a WFS709TP's basic SNMP parameters:

1. Configure the host name by navigating to the Configuration > Basic > Management > SNMP page on the browser interface (Figure 13-1).

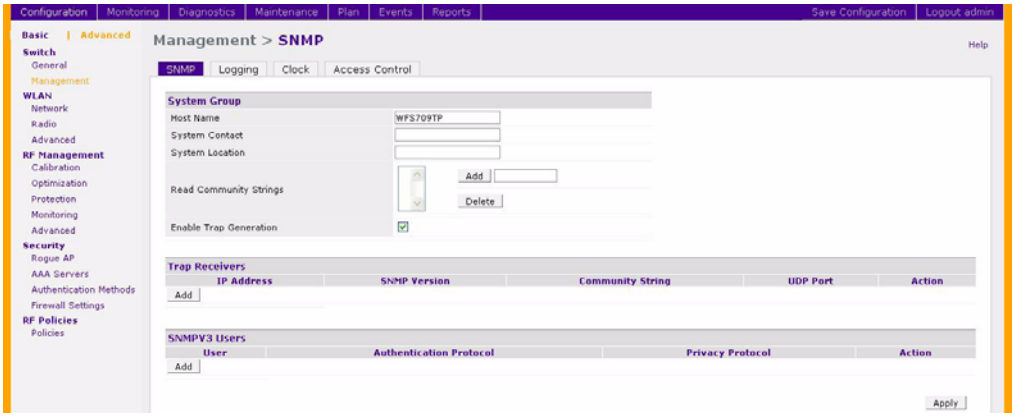

Figure 13-1

2. Enter the parameters described in Table 13-1.

Table 13-1. Basic WFS709TP SNMP Parameters

Field	Description	Expected/Recommended Value
Host Name	Host name of the WFS709TP.	String to act as the host name for the WFS709TP being configured.
System Contact	Person who acts as the System Contact or administrator for the WFS709TP.	System contact's name and contact information.
System Location	Location of the WFS709TP.	String to describe the location of the WFS709TP.

Table 13-1. Basic WFS709TP SNMP Parameters (continued)

Field	Description	Expected/Recommended Value
Read Community Strings	Community strings used to authenticate requests for SNMP versions before version 3.	These are the community strings that are allowed to access the SNMP data from the WFS709TP (only needed if using SNMP v2c).
Enable Trap Generation	Enables generation of SNMP traps to configured SNMP trap receivers. Refer to "SNMP Traps" on page 13-9 for a list of traps that are generated by the WFS709TP.	Select this option and configure the details of the trap receivers to enable generation of traps for various events by the WFS709TP.
Trap receivers	Host information about a trap receiver. This host must be running a trap receiver to receive and interpret the traps sent by the WFS709TP.	Configure the following for each host/trap receiver: • IP address. • SNMP version (1 or 2c). • Community string. • (Optional) UDP port on which the trap receiver is listening for traps. The default is the UDP port number 162.

If you are using SNMPv3 for getting the values from the WFS709TP, follow the steps below to configure valid users for SNMPv3:

1. Click Add in the SNMPv3 Users section to add a new SNMPv3 user.
2. Enter the information described in Table 13-2.

Table 13-2. SNMPv3 User Details

Field	Description	Expected/Recommended Value
User name	A string representing the name of the user.	A string value for the user name.
Authentication protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol being used.	This can take one of the two values: • MD5: HMAC-MD5-96 Digest Authentication Protocol • SHA: HMAC-SHA-96 Digest Authentication Protocol
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol.	String password for MD5 or SHA, depending on the choice of protocol.

Table 13-2. SNMPv3 User Details (continued)

Field	Description	Expected/Recommended Value
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol being used.	This takes the value DES (CBC-DES Symmetric Encryption Protocol).
Privacy protocol password	If messages sent on behalf of this user can be encrypted/decrypted, the (private) privacy key for use with the privacy protocol.	String password for DES.

SNMP for Access Points

Access points also support SNMP. The administrator can configure all or some of the APs to access data using SNMP as well as receive traps from the APs. The APs can be acting as Air Monitors (AMs) when they are used to access information about the wireless network using SNMP. The SNMP configuration for the APs can be done at a global level (thereby being applicable for all the APs in the network), or for a particular set of APs by using the AP location codes.

Note: The configuration for access points is always done on the master WFS709TP only.

To configure SNMP parameters for access points in the network at a global level:

1. Navigate to the Configuration > Advanced > WLAN > Network > General page of the master WFS709TP (Figure 13-2). This page includes fields for configuring the SNMP parameters on all access points in the network.

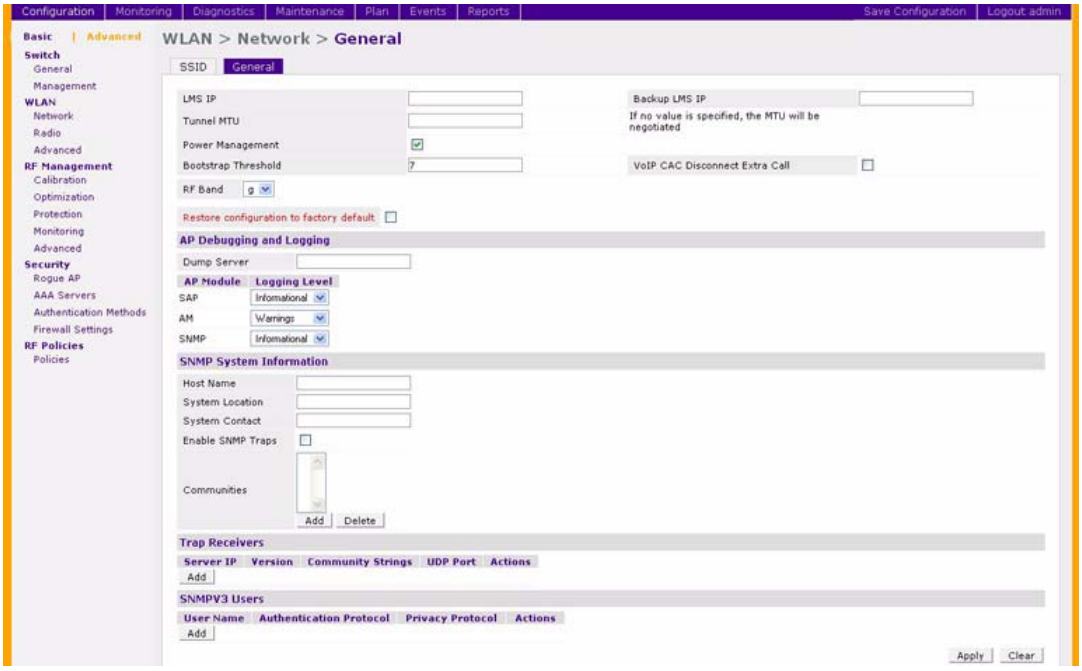

Figure 13-2

2. Configure the basic SNMP parameters in the SNMP System Information area. The fields are similar to those for the WFS709TP, and are explained in Table 13-3.

Table 13-3. Basic Access Point SNMP Parameters

Field	Description	Expected/Recommended Values
Host Name	Host name for all Access Points in the network.	A name to identify the devices as WFS709TP APs.
System Location	Location for Access Points in the network.	String to identify the location of the APs.
System Contact	Contact name or information for administrative contact.	String to identify administrative contact for all APs.

Table 13-3. Basic Access Point SNMP Parameters (continued)

Field	Description	Expected/Recommended Values
Enable SNMP Traps	Enables generation of SNMP traps from all Access Points. Refer to "SNMP Traps" on page 13-9 for a complete list of traps that may be generated by access points in the network.	Select this option to enable generation of traps. Ensure that at least one trap receiver is configured to complete the traps configuration.
Communities	Community strings used to authenticate requests for SNMP versions before version 3.	These are the community strings that are allowed to access the SNMP data from the WFS709TP (only needed if using SNMP v2c).
Trap receivers	Host information about a trap receiver. This host must be running a trap receiver to receive and interpret the traps sent by the access points.	Configure the following for each host/ trap receiver: • IP address. • SNMP version (1 or 2c). • Community string. • (Optional) UDP port on which the trap receiver is listening for traps. The default is the UDP port number 162.

3. If you are using SNMPv3 for getting the values from the WFS709TP, refer to Table 13-4 to configure valid users for SNMPv3.

Table 13-4. SNMPv3 Access Point User Details

Field	Description	Expected/Recommended Values
User name	A string representing the name of the user.	A string value for the user name.
Authentication protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol that is used.	This can take one of two values: • MD5: HMAC-MD5-96 Digest Authentication Protocol. • SHA: HMAC-SHA-96 Digest Authentication Protocol.
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol.	String password for MD5 or SHA, depending on the choice of protocol.

Table 13-4. SNMPv3 Access Point User Details (continued)

Field	Description	Expected/Recommended Values
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol that is used.	This takes the value DES (CBC-DES Symmetric Encryption Protocol).
Privacy protocol password	If messages sent on behalf of this user can be encrypted/decrypted, the (private) privacy key for use with the privacy protocol.	String password for DES.

All the parameters listed in Table 13-4 can also be configured for a subset of all the access points in the network by using the location code of the access points in the *building.floor.location* format. The administrator can use 0 as the wild card value for any of the fields in this format. As an example, all APs in building 10 can be represented by the location code *10.0.0*. To configure the SNMP parameters for a set of APs, follow these steps:

1. Navigate to the Configuration > Advanced > WLAN > Advanced page on the browser interface of the master WFS709TP.
2. Determine if the required AP set already exists.
   - If the required set does not exist, click Add to add the set of APs represented by a location code, using 0 as the wild card value when required.(Figure 13-3).
   - If the set already exists, click Edit for the chosen set and proceed to step 4 to configure the SNMP parameters for the chosen set.

Figure 13-3

3. Navigate to Configuration > Advanced > WLAN > Network > SSID to configure the SSID for the added APs (Figure 13-4).

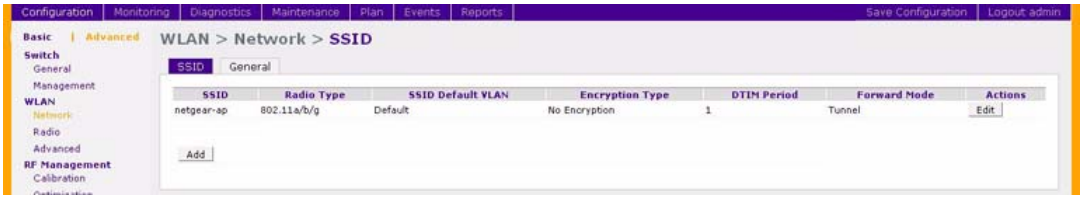

Figure 13-4

4. Click the General tab to configure the SNMP parameters for the set of APs (Figure 13-5).

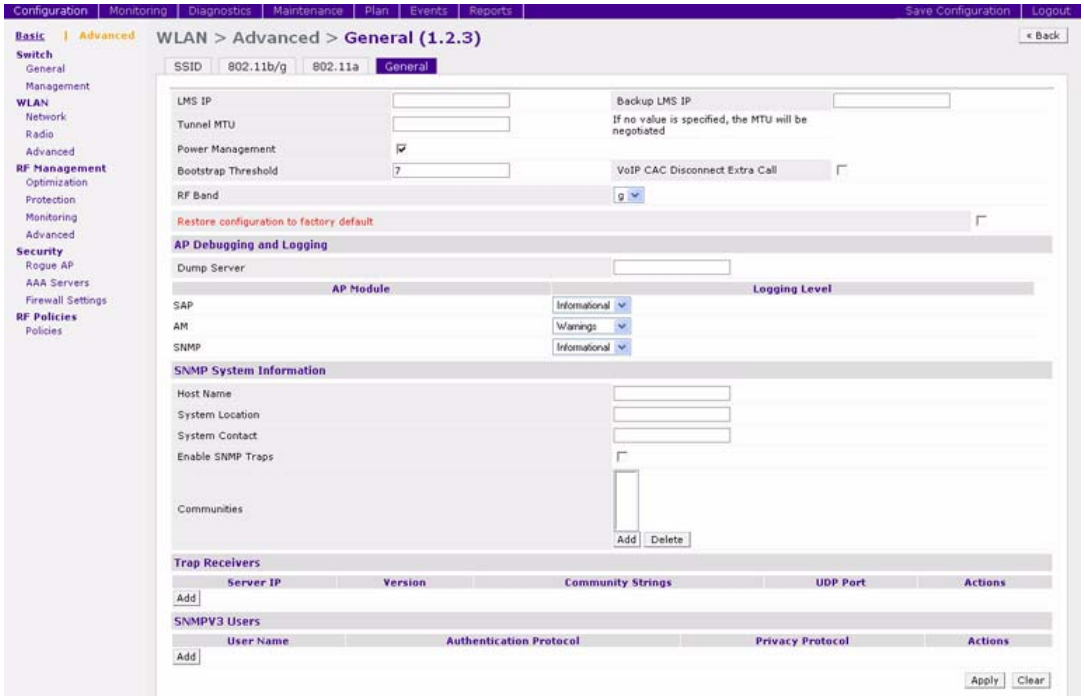

Figure 13-5

5. Refer to Table 13-3 and Table 13-4 for the fields to be configured for the set of APs.
6. Click Apply to apply the configuration.

SNMP Traps

WFS709TP Traps

Table 13-5 lists the key traps generated by the WFS709TP.

Table 13-5. WFS709TP SNMP Traps

Trap	Description	Priority Level
WFS709TP IP changed	The WFS709TP IP has been changed. The WFS709TP IP is either the loopback IP address or the IP address of the VLAN 1 interface (if no loopback IP address is configured).	Critical
WFS709TP role changed	The WFS709TP has transitioned from being a master WFS709TP to a local WFS709TP, or vice versa.	Critical
User entry created/ deleted/authenticated/ de-authenticated/ authentication failed	Each of these traps is triggered by an event related to a user event. The event can be a new user entry being created in the user table, deletion of a user entry, a user getting authenticated successfully, a user getting de-authenticated, or a failed authentication attempt.This is a local event to the WFS709TP where the user is visible, and each of these traps will be generated by the WFS709TP on which the user event occurs.	Medium.
Authentication server request timed out	A request to a authentication server did not receive a response from the server within a specified amount of time, and therefore the request timed out. This usually indicates a connectivity problem from the WFS709TP to the authentication server or some other problem related to the authentication server.	High.
Authentication server timed out	An authentication server has been taken out of service. This trap is almost always same as AuthServerReqTimedOut except when there is only one authentication server, in which case the server will never be taken out of service.	High
Authentication server up	An authentication server that was previously not responding has started responding to authentication requests. This trap will be triggered by a user event that causes the WFS709TP to send an authentication request to the authentication server.	Low.
Authentication user table full	The authentication user table has reached its limit of the number of user entries it can hold. This event is local to the WFS709TP that generates the traps. The maximum number of user entries that can be present at the same time in the user table is 4096.	Critical.
Authentication Bandwidth contracts table full	The maximum number of configured bandwidth contracts on the WFS709TP has been exceeded. The threshold is 4096.	High

Table 13-5. WFS709TP SNMP Traps (continued)

Trap	Description	Priority Level
Authentication ACL table full	The maximum number of ACL entries in the ACL table has been exceeded. The limit is 2048 entries on a WFS709TP.	High
Power supply failure	One of the two possible power supplies in the WFS709TP has failed.	Critical
Fan failure	The fan in the WFS709TP has failed.	Critical
Out of Range Voltage	An out-of-range voltage is being supplied to the WFS709TP.	Critical
Out of Range temperature	An out-of-range operating temperature being supplied to the WFS709TP.	Critical
Line card inserted/ removed	A Line Card has been inserted or removed from the WFS709TP.	Critical
Supervisor card inserted/ removed	A Supervisor card has been inserted or removed from the WFS709TP.	Critical
Power supply missing	One of the power supplies is missing.	Critical

Access Point/Air Monitor Traps

Table 13-6 lists the key traps generated by an access point or an air monitor,

Table 13-6. Access Point SNMP Traps

Trap	Description	Priority Level
Unsecure AP detected	An AM has detected and classified an AP as unsecure. This trap will indicate the location of the AM that has detected the unsecure AP, the channel on which the AP was detected, and the BSSID and SSID of the detected AP.	Critical
Station impersonation	An AM has detected a Station impersonation event. The trap will provide the location of the AM that has detected the event and the MAC address of the Station.	Critical
Reserved channel impersonation	An AP is being detected is violating the Reserved Channels. This trap will indicate the location of the AP or AM that detects the event, and the BSSID and SSID of the detected AP.	High
Valid SSID violation	This trap indicates a violation in the configuration of the SSID of the AP. The AP generates the trap and includes its BSSID, the configured SSID, and the location of the AP in the trap.	High
Channel misconfiguration	This trap indicates an error in channel configuration of an AP. The AP generates the trap and includes its BSSID, the configured SSID, and the location of the AP in the trap.	High

Table 13-6. Access Point SNMP Traps (continued)

Trap	Description	Priority Level
OUI misconfiguration	This trap indicates an error in the Organizationally Unique Identifier (OUI) configuration of an AP. The AP generates the trap and includes its BSSID, the configured SSID, and the location of the AP in the trap.	High
SSID misconfiguration	This trap indicates an error in the SSID configuration of an AP. The AP generates the trap and includes its BSSID, the configured SSID, and the location of the AP in the trap.	High
Short Preamble misconfiguration	This trap indicates an error in the Short Preamble configuration of an AP. The AP generates the trap and includes its BSSID, the configured SSID, and the location of the AP in the trap. This check will be done only if the short-preamble option is selected for the AP from the browser interface.	High
AM misconfiguration	This trap indicates an error in the Short Preamble configuration of an AP. The AP generates the trap and includes its BSSID, the configured SSID, and the location of the AP in the trap.	High
Repeat WEP-IV violation	The AM has detected a valid station or a valid AP sending consecutive frames that have the same initialization vector (IV). This usually means that entity has a “flawed” WEP implementation and is therefore a potential security risk.	High
Weak WEP-IV violation	The AM has detected a valid station or a valid AP sending frames with an IV that is in the range of IVs that are known to be cryptographically weak and therefore are a potential security risk.	High.
Adhoc networks detected	The AM has detected Adhoc networks.	High
Valid station policy violation	A valid Station policy is being violated.	High
AP interference.	The indicated AM (identified by the BSSID/ SSID) is detecting AP interference on the indicated channel.	Medium
Frame Retry rate exceeded	The percentage of received and transmitted frames with the retry bit has crossed the High watermark. This event can be triggered for an AP, a station, or a channel. The two values that should be configured related to this event are Frame Retry Rate – High Watermark and Frame Retry Rate –Low Watermark. *	Medium

Table 13-6. Access Point SNMP Traps (continued)

Trap	Description	Priority Level
Frame Bandwidth rate exceeded	This trap refers to the event of the bandwidth rate for a station exceeding a configured threshold (High Watermark).	Medium
Frame low speed rate exceeded	This trap refers to the event when the percentage of received and transmitted frames at low speed (less that 5.5Mbps for 802.11b and less that 24 Mbps for 802.11a) exceeds the configured High Watermark.	Medium

* The High Watermark refers to the percentage threshold, which if surpassed triggers the event that causes the trap to be sent. The Low Watermark refers to the percentage threshold, such that if the retry rate reaches a value lower than this value the event is reset. The trap will be triggered the first time the Frame Retry rate crosses the High Watermark and then will only be triggered if the Frame Retry Rate goes under the Low Watermark and then crosses the High Watermark again. This holds true for the bandwidth rate and low speed rate thresholds as well.

Configuring Logging

This section outlines the steps required to configure logging on an WFS709TP. The logging level can be set for each of the modules in the software system. Table 13-7 summarizes these modules.

Table 13-7. WFS709TP Modules

Module	Description
Authentication	The module responsible for authentication of wireless clients
Configuration Manager	The module responsible for configuration changes in the network and configuration synchronization among all WFS709TPs
Management AAA	The module responsible for authentication of management users (telnet/ssh/WebUI)
DHCP server	The DHCP server in the WFS709TP
Switching	The module responsible for all Layer 2/3 switching functionality
Mobility	The module responsible for inter-WFS709TP and intra-WFS709TP mobility for wireless clients
Access Point Manager	The module responsible for managing the APs in the network
Station Manager	The module responsible for all wireless stations at a 802.11 level
Traffic	A logical module to track traffic patterns to help troubleshooting

You can configure the logging levels for each of these modules as well as the IP address of a syslog server to which the WFS709TP can direct these logs. To configure logging:

1. Navigate to the Configuration > Advanced > Switch > Management > Logging page on the browser interface (Figure 13-6).

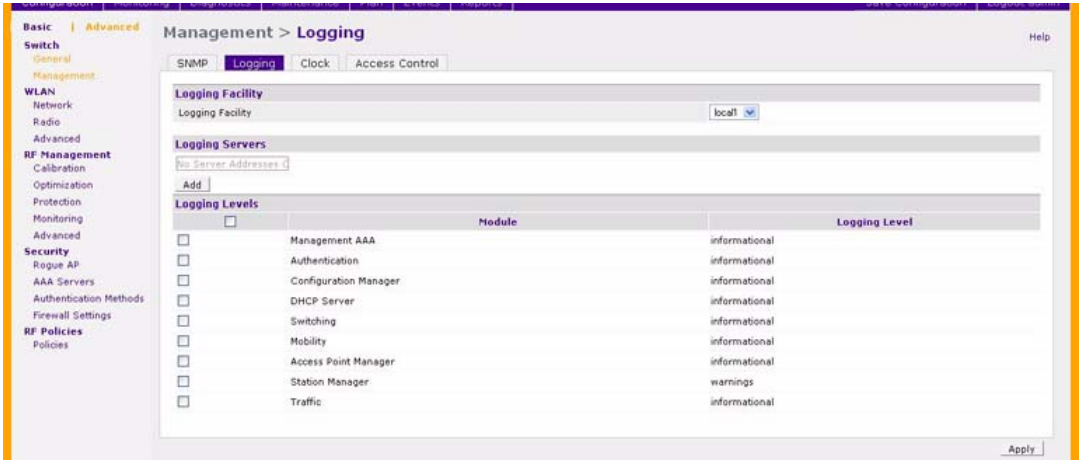

Figure 13-6

2. To add a logging server, click Add in the Logging Server section.
3. Click Add to add the logging server to the list of logging servers. Ensure that the syslog server is enabled and configured on this host.
4. Determine if the logging levels are set as required.
   - If the logging levels of all the modules are set as required, proceed to step 6.
   - To modify the logging level of any of the modules, select the required module from the list of the modules shown. From the drop-down list that appears on the screen, choose the appropriate logging level.

In the example shown in Figure 13-7, the logging level of the Authentication and VPN server module is being modified to debugging.

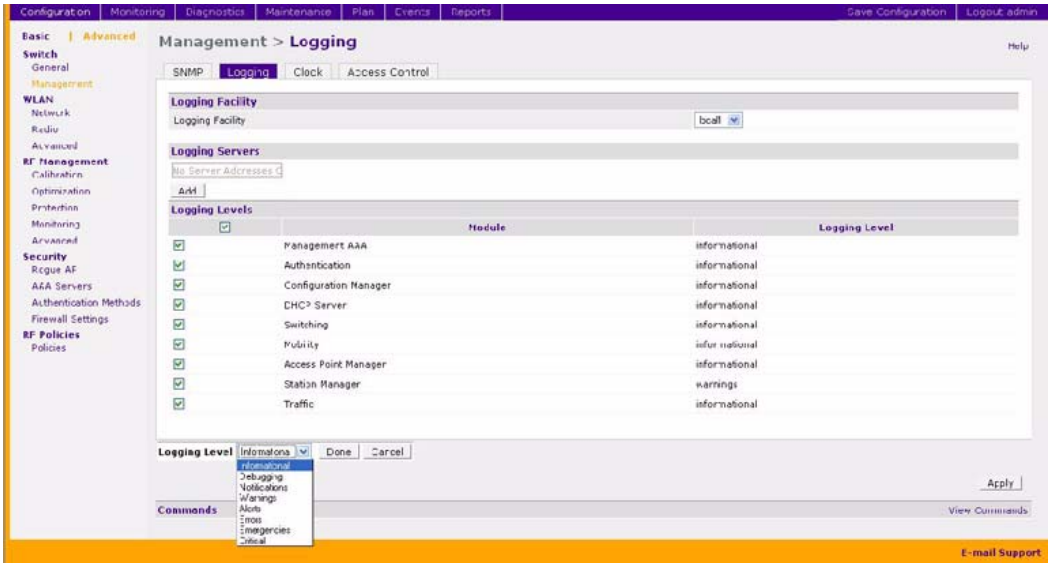

Figure 13-7

5. Click Done to make the modification.
6. Click Apply to apply the configuration.

Creating Guest Accounts

You can create a special administrative login that allows a user, such as a front desk receptionist, to create guest accounts on a browser interface page.

To create the user login:

1. Navigate to the Configuration > Basic > Management > Access Control page.
2. Click Add.
3. In the Add User page (Figure 13-8), enter the name that the user will log in with to access the guest account page.
4. Enter the password for the user login.

5. For Role, select guest-provisioning from the drop-down list.

Figure 13-8

6. Click Apply.

When a user logs into the browser interface on the WFS709TP (in a multi-switch system, this must be the master WFS709TP) using the login and password you just created:

1. A special browser interface page is displayed that allows them to create guest accounts in the WFS709TP's internal database (Figure 13-9).

Figure 13-9

2. The user clicks Add to create a guest account (Figure 13-10):

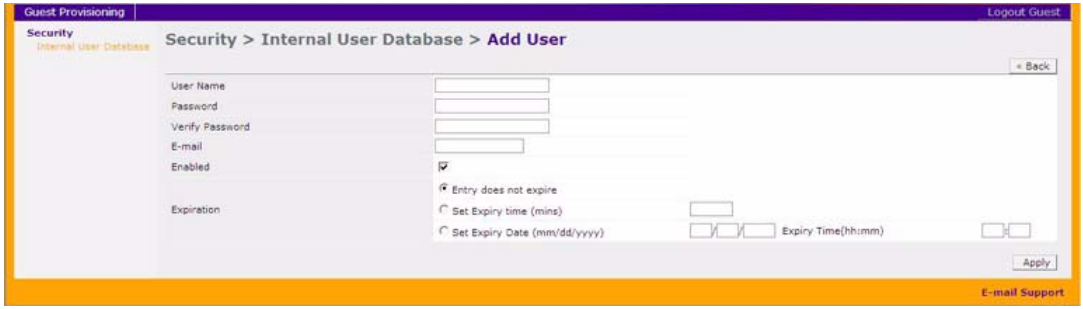

Figure 13-10

3. The user can then define a user name and password for the guest account and configure the expiration for the account. Clicking Apply adds the guest account to the database (Figure 13-11). The user can then disable, delete, or modify the guest account as needed.

Figure 13-11

Managing Files on the WFS709TP

You can transfer these types of files between the WFS709TP and an external server or host:

- A WFS709TP operating system (OS) image file
- A specified file in the WFS709TP's flash file system, or a compressed archive file that contains the entire content of the flash file system

> **Note:** You back up the entire content of the flash file system to a compressed archive file, which you can then copy from the flash system to another destination.

- A configuration file, either active running configuration or startup configuration
- Log files

Table 13-8 lists the external servers that you can use to copy files to or from a WFS709TP.

Table 13-8. Servers for File Transfer

Server Type	Configuration
Trivial File Transfer Protocol (TFTP)	• IP address of the server
File Transfer Protocol (FTP)	• IP address of the server • Username and password to log into server
Secure Copy (SCP)	• IP address of the server • Username and password to log into server

Note: you cannot copy log files with SCP; the file must be an image, flash, or configuration file.

For example, you can copy an OS image file from an SCP server to a system partition on a WFS709TP or copy the startup configuration on a WFS709TP to a file on a TFTP server. You can also store the contents of a WFS709TP's flash file system to an archive file that you can then copy to an FTP server.

Managing Image Files

You can upload an OS image file onto a WFS709TP from a TFTP, FTP, or SCP server. In addition, the browser interface allows you to upload an OS image file from the local computer on which you are running the browser.

When you transfer an OS image file, you must specify the system partition to which the file is copied.

To transfer OS image files:

1. Navigate to the Maintenance > Switch > Image Management page.
2. Select TFTP, FTP, SCP, or Upload Local File.
3. Enter or select the appropriate values for the method.
4. Select the system partition to which the image file is copied.
5. Specify the boot partition, whether the switch is to be rebooted after the image file is transferred, and whether the current configuration is saved before the switch is rebooted.
6. Click Upgrade.

Backing Up and Restoring the Flash File System

You can store the entire content of the flash file system on a WFS709TP to a compressed archive file. You can then copy the archive file to an external server for backup purposes. If necessary, you can restore the backup file from the server to the flash file system.

To create and copy a backup of the flash file system:

1. Navigate to the Maintenance > File > Backup Flash page.
2. Click Create Backup to back up the contents of the flash system to the flashbackup.tar.gz file.

3. Click Copy Backup to enter the Copy Files page where you can select the destination server for the file.
4. Click Apply.

To restore the backup file to the flash file system:

1. Navigate to the Maintenance > File > Copy Files page.
   a. For Source Selection, specify the server to which the flashbackup.tar.gz file was previously copied.
   b. For Destination Selection, select Flash File System.
   c. Click Apply.
2. Navigate to the Maintenance > File > Restore Flash page.
3. Click Restore to restore the flashbackup.tar.gz file to the flash file system.
4. Navigate to the Maintenance > Switch > Reboot Switch page.
5. Click Continue to reboot the WFS709TP.

Copying Log Files

You can copy log files from the WFS709TP to an external TFTP or FTP server. The browser interface allows you to copy the log files to a WinZip folder, which you can display or save on your local PC.

To copy log files:

1. Navigate to the Maintenance > File > Copy Logs page.
2. For Destination, specify the TFTP or FTP server to log files are copied.
3. Select Download Lgs to download the log files into a WinZip file on your local PC.
4. Click Apply.

Copying Other Files

You can copy a file in the flash file system or a configuration file between the WFS709TP and an external server.

To copy a file:

1. Navigate to the Maintenance > File > Copy Files page.
2. Select the source where the file or image exists.

3. Select the destination to where the file or image is to be copied.
4. Click Apply.

Installing a Server Certificate

Captive Portal and IEEE 802.1x with AAA FastConnect require that you install a server certificate in the WFS709TP (see "802.1x Authentication" on page 7-1 and "Overview of Captive Portal Functions" on page 8-1). There is a default server certificate installed in the WFS709TP, however this certificate does not guarantee security for production networks. NETGEAR strongly recommends that you replace the default server certificate in the WFS709TP with a custom certificate issued for your site or domain by a trusted certificate authority (CA).

To obtain a security certificate for the WFS709TP, generate and submit a Certificate Signing Request (CSR) to the CA of your choice. Upon receiving the CA-signed server certificate, install the certificate from your PC as described in this section.

Certificates must be in X.509 PEM format.

To install a server certificate in the WFS709TP:

1. Navigate to the Maintenance > Captive Portal > Upload Certificate page.
2. Click Browse to specify the location of the certificate on your PC.
3. Click Upload.

Note: Certificate installation shuts down web server connections.

Chapter 14
Configuring WFS709TP for Voice

This chapter outlines the steps required to configure a WFS709TP ProSafe Smart Wireless Switch for voice devices, including SIP phones and SVP phones. Since voice applications are more vulnerable to delay and jitter, the network infrastructure should be able to prioritize the voice traffic over the data traffic. This chapter also describes voice-related features that you can configure in the WFS709TP operating system.

It includes the following topics:

Voice over IP Proxy ARP

You can enable proxy address resolution protocol (ARP) on the WFS709TP for voice over IP (VoIP) clients. When the WFS709TP receives an ARP broadcast for a VoIP client, the switch constructs an ARP response containing the client's MAC address.

This feature reduces the number of broadcast packets sent to VoIP clients, thereby improving the battery life of voice handsets. You can enable this option for voice handsets in conjunction with increasing the Delivery Traffic Indication Message (DTIM) interval on clients.

To enable the VoIP proxy ARP feature for VoIP clients:

1. Navigate to the Configuration > Advanced > Security > Firewall Settings page.
2. Select VOIP Proxy ARP.
3. Click Apply.

Battery Boost

Battery boost converts all multicast traffic to unicast before delivery to the client. This feature is disabled by default. Enabling battery boost on an SSID allows you to set the DTIM interval from 10 to 100, equating to 1,000–10,000 milliseconds. This longer interval keeps associated wireless clients from activating their radios for multicast indication and delivery, leaving them in power-save mode longer, and thus lengthening battery life. The DTIM configuration is performed on the WLAN, so no configuration is necessary on the client. Although the multicast-to-unicast conversion generates more traffic, that traffic is buffered by the AP and delivered to the client when the client emerges from power-save mode.

An associated parameter available on some clients is the Listening Interval (LI), which defines the interval (in number of beacons) after which the client must wake to read the Traffic Indication Map (TIM). The TIM indicates whether there is buffered unicast traffic for each sleeping client. With battery boost enabled, the DTIM is increased but multicast traffic is buffered and delivered as unicast. Increasing the LI can further increase battery life, but can also decrease client responsiveness. NETGEAR recommends a DTIM setting of 10 or less for NEC FOMA N900iL clients, and 30 or less for BlackBerry 7270 clients.

You enable the battery boost feature and set the DTIM interval in the WLAN configuration.

To enable battery boost:

1. Navigate to the Configuration > Advanced > WLAN > Advanced page.
2. Click Add to add a new location.
3. Enter a location ID in the format *building.floor.plan*, where each value is an integer.
4. Click Add.
5. Select the 802.11b/g or 802.11a tab to configure radio settings.
6. Select Battery Boost.
7. Configure the DTIM Period if needed.
8. Click Apply.

Limiting the Number of Active Voice Calls

You can limit the number of active voice calls allowed on a radio. This feature is disabled by default. When the disconnect extra call feature is enabled, the system monitors the number of active voice calls, and if the defined threshold is reached, any new calls are disconnected. The AP denies association requests from a device that is on call.

You enable this feature in the WLAN configuration. You also need to enable call admission control, which is disabled by default. You can also configure the number of simultaneous calls that a radio can handle on a per-protocol basis.

To limit the number of active voice calls:

1. Navigate to the Configuration > Advanced > WLAN > Advanced page.
2. Click Add to add a new location.
3. Enter a location ID in the format *building.floor.plan*, where each value is an integer.
4. Click Add.
5. Select the General tab.
6. Select VoIP CAC Disconnect Extra Call.
7. Click Apply.
8. Select the 802.11b/g or 802.11a tab to configure radio settings.
9. Scroll to the bottom of the page to display VoIP parameters.
10. Select VoIP Call Admission Control.
11. Configure the Call Capacity for the VoIP protocol if needed.
12. Click Apply.

WPA Fast Handover

In 802.1x authentication, the WPA fast handover feature allows certain WPA clients to use a pre-authorized Pairwise Master Key (PMK), significantly reducing handover interruption. Check with the manufacturer of your handset to see if this feature is supported. This feature is disabled by default.

Note: This feature supports WPA clients, while opportunistic key caching (also configured in 802.1x authentication) supports WPA2 clients.

To enable WPA fast handover:

1. Navigate to the Configuration > Advanced > Security > Authentication Methods > 802.1x page.
2. Under Advanced Configuration, select Show.
3. Select WPA FastHandover.
4. Click Apply.

Appendix A
Configuring DHCP with Vendor-Specific Options

A standards-compliant DHCP server can be configured to return the host WFS709TP ProSafe Smart Wireless Switch's IP address through the Vendor-Specific Option Code (option 43) in the DHCP reply. In the WFS709TP system, this information can allow a NETGEAR access point to automatically discover the IP address of a master WFS709TP for its configuration and management.

This appendix describes how to configure vendor-specific option 43 on various DHCP servers. It includes the following topics:

Overview

DHCP servers are a popular way of configuring clients with basic networking information such as IP address, default gateway, network mast, and DNS server. Most DHCP servers have the ability to also send a variety of optional information, including the Vendor-Specific Option Code, also called option 43.

Here is how option 43 works for the WFS709TP:

1. The DHCP client on a WFS709TP AP adds an optional piece of information called the Vendor Class Identifier Code (option 60) to its DHCP request. The value of this code is **NetgearAP**.
2. The DHCP server sees the Vendor Class Identifier Code in the request and checks to see if it has option 43 configured. If it does, it sends the Vendor-Specific Option Code (option 43) to the client. The value of this option is the loopback address of the master WFS709TP.
3. The AP receives a response from the DHCP server and checks if option 43 is returned. If it is, the AP contacts the master WFS709TP using the supplied IP address.

Windows-Based DHCP Servers

Configuring a Microsoft Windows-based DHCP server to send option 43 to the DHCP client on an AP connected to a WFS709TP consists of two tasks:

- Configuring Option 60
- Configuring Option 43

Configuring Option 60

The Vendor Class Identifier Code (option 60) identifies and associates a DHCP client with a particular vendor. Any DHCP server configured to take action based on a client's vendor ID should also have this option configured. Since option 60 is not a predefined option on a Windows DHCP server, you must add it to the option list for the server.

To configure option 60 on the Windows DHCP server:

1. On the DHCP server, open the DHCP server administration tool by clicking Start > Administration Tools > DHCP.
2. Find your server and right-click on the scope to be configured under the server name. Select Set Predefined Options.
3. In the Predefined Options and Values dialog box, click the Add button.
4. In the Option Type dialog box, enter the following information:
   - Name: Netgear Access Point
   - Data Type: String
   - Code: 60
   - Description: Netgear AP vendor class identifier
5. Click OK to save this information.
6. In the Predefined Options and Values dialog box, make sure 060 Netgear Access Point is selected from the Option Name drop-down list.
7. In the Value field, enter the following information:

   String: Netgear Access Point
8. Click OK to save this information.

Configuring Option 43

Option 43 returns the IP address of the master WFS709TP to a DHCP client. This information allows the APs to auto-discover the master WFS709TP and obtain their configuration.

To configure option 43 on the Windows DHCP server:

1. On the DHCP server, open the DHCP server administration tool by clicking Start > Administration Tools > DHCP.
2. Find your server and right-click on the scope to be configured under the server name. Click on the Scope Options entry and select Configure Options.
3. In the Scope Options dialog box (Figure A-1), scroll down and select 043 Vendor Specific Info.

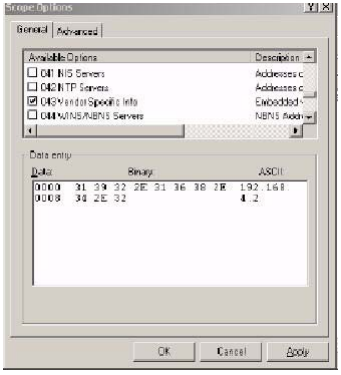

Figure A-1

4. In the Data Entry field, click anywhere in the area under the ASCII heading and enter the following information:

   ASCII: Loopback address of the master WFS709TP

5. Click OK to save the configuration.

Option 43 is configured for this DHCP scope. Note that even though you entered the IP address in ASCII text, it displays in binary form (Figure A-2).

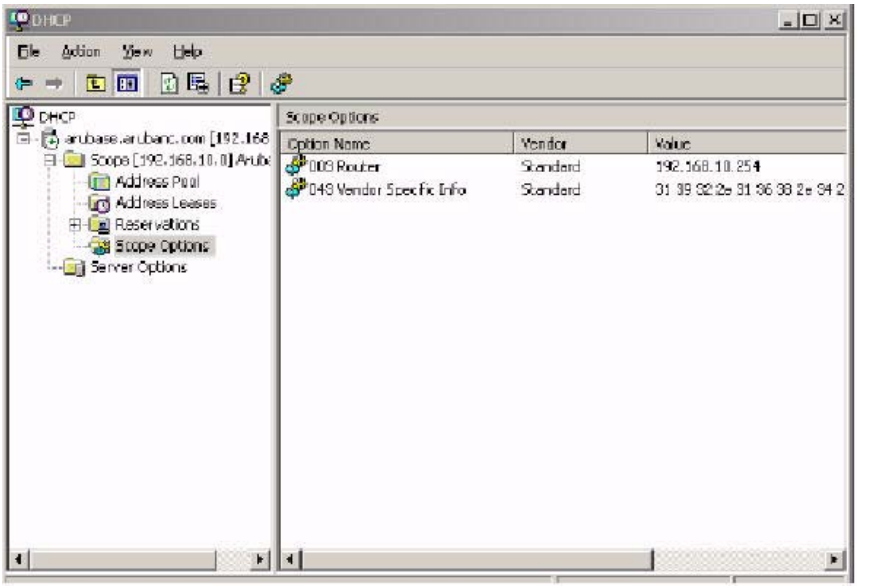

Figure A-2

Linux DHCP Servers

The following code is an example configuration for the Linux dhcpd.conf file.

	Note: After you enter the configuration, you must restart the DHCP service.

```
option serverip code 43 = ip-address;
class "vendor-class" {
      match option vendor-class-identifier;
}
.
.
.
```

```
subnet 10.200.10.0 netmask 255.255.255.0 {
   default-lease-time 200;
   max-lease-time 200;
   option subnet-mask 255.255.255.0;
   option routers 10.200.10.1;
   option domain-name-servers 10.4.0.12;
   option domain-name "vlan10.aa.netgear.com";
   subclass "vendor-class" "NetgearAP" {
      option vendor-class-identifier "NetgearAP";
      option serverip 10.200.10.10;
   }
   range 10.200.10.200 10.200.10.252;
}
```

Appendix B
Windows Client Example Configuration for 802.1x

This appendix provides an example configuration for a wireless client (the 802.1x supplicant) in a Windows environment.

	**Note:** For detailed information about configuring computers in a Windows environment for PEAP-MS-CHAPv2 and EAP-TLS authentication, see the Microsoft document "Step-by-Step Guide for Setting Up Secure Wireless Access in a Test Lab," available from Microsoft's Download Center at *http://www.microsoft.com/downloads.*

Window XP Wireless Client Example Configuration

This section shows an example of how to configure a Windows XP wireless client using Windows XP's Wireless Zero Configuration service.

	**Note:** The following steps apply to a computer running Windows XP Professional Version 2002 with Service Pack 2. To configure a wireless client on other Windows platforms, see your Microsoft Windows documentation

1. On the desktop, right-click My Network Places and select Properties.
2. In the Network Connections window, click Wireless Network Connection and select Properties.
3. Select the Wireless Networks tab.

This screen displays the available wireless networks and the list of preferred networks (Figure B-1). Windows connects to the preferred networks in the order in which they appear.

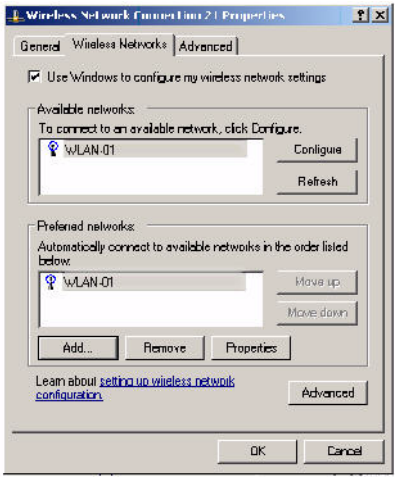

Figure B-1

4. Click the Advanced button to display the Networks to access window (Figure B-2).

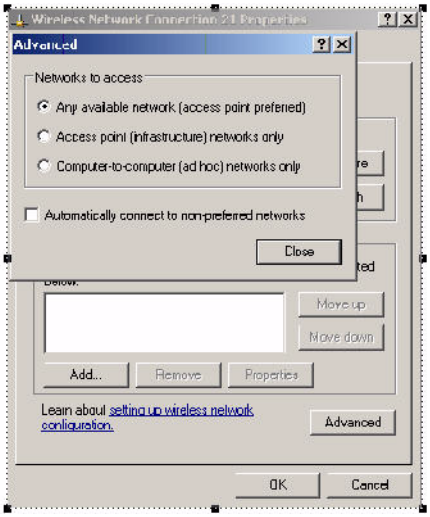

Figure B-2

This window determines what types of wireless networks the client can access. By default, Windows connects to any type of wireless network.

5. Make sure that the option Computer-to-computer (ad hoc) networks only is *not* selected, then click Close.
6. In the Wireless Networks tab, click Add to add a wireless network.
7. Click the Association tab to enter the network properties for the ESSID.

   This tab configures the authentication and encryption used between the wireless client and the WFS709TP system. Therefore, the settings for the ESSID that you configure on the client must match the configuration for the ESSID on the WFS709TP.

   - For an SSID using dynamic WEP, enter the following:
     - Network Authentication: Open
     - Data Encryption: WEP
     - Select the option “The key is provided for me automatically”.

     Each client will use a dynamically generated WEP key that is automatically derived during the 802.1x process.
   - For an SSID using WPA, enter the following:
     - Network Authentication: WPA
     - Data Encryption: TKIP
   - For an SSID using WPA-PSK, enter the following:
     - Network Authentication: WPA-PSK
     - Data Encryption: TKIP
     - The preshared key.
   - For an SSID using WPA2, enter the following:
     - Network Authentication: WPA2
     - Data Encryption: AES
   - For an SSID using WPA2-PSK, enter the following:
     - Network Authentication: WPA2-PSK
     - Data Encryption: AES
     - The preshared key.

     Do *not* select the option “This is a computer-to-computer (ad hoc) network; wireless access points are not used”.

Figure B-3 shows the configuration for the ESSID WLAN-01 that uses dynamic WEP.

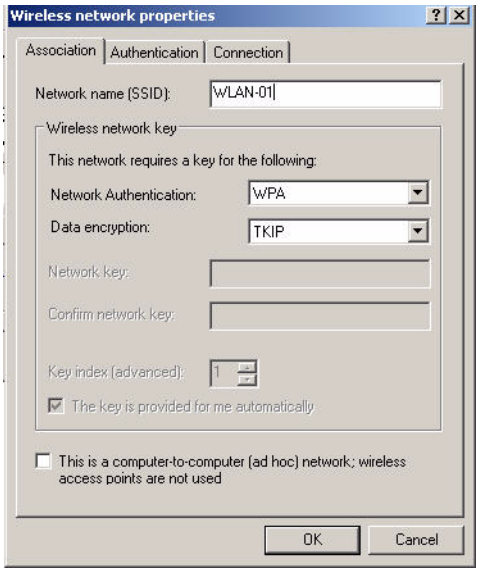

Figure B-3

8. Click the Authentication tab to enter the 802.1x authentication parameters for the ESSID.

This tab configures the EAP type used between the wireless client and the authentication server.

9. Configure the following, as shown in Figure B-4:

- Select Enable IEEE 802.1x authentication for this network.
- Select Protected EAP (PEAP) for the EAP type.
- Choose the authentication type.
  - Select Authenticate as computer when computer information is available. The client will perform computer authentication when a user is not logged in.
  - Do not select Authenticate as guest when user or computer information is unavailable. The client will not attempt to authenticate as a guest.

.

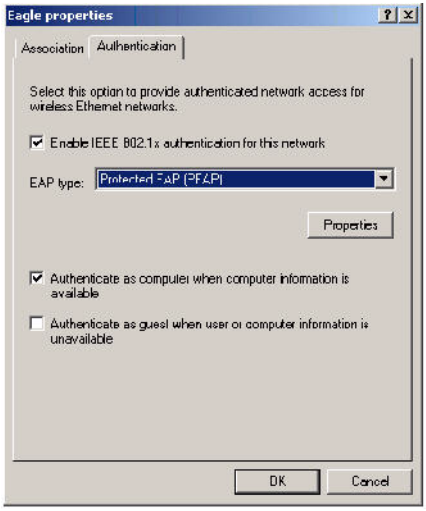

Figure B-4

10. Under EAP type, select Properties to display the Protected EAP Properties window. Configure the client PEAP properties, as shown in Figure B-5:

- Select Validate server certificate. This instructs the client to check the validity of the server certificate from an expiration, identity, and trust perspective.
- Select the trusted Certification Authority (CA) that can issue server certificates for the network.
- Select Secured password (EAP-MSCHAP v2). The PEAP “inner authentication” mechanism will be an MS-CHAPv2 password.

- Select Enable Fast Reconnect to speed up authentication in some cases.

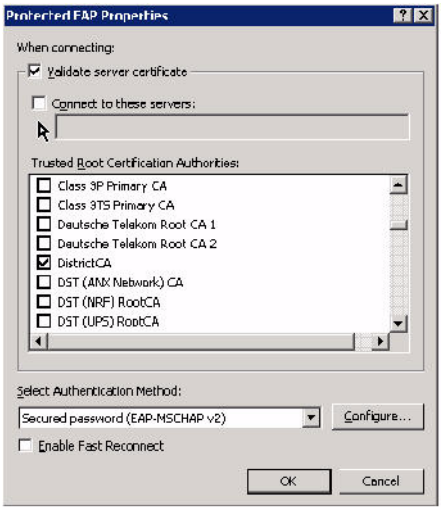

Figure B-5

11. Under Select Authentication Method, click Configure to display the EAP-MSCHAPv2 Properties window. Select the option Automatically use my Windows logon name and password, and domain if any (Figure B-6).

This option specifies that the user's Windows logon information is used for authentication to the wireless network. This option enables single sign-on, allowing the same logon to be used for access to the Windows domain as well as the wireless network.

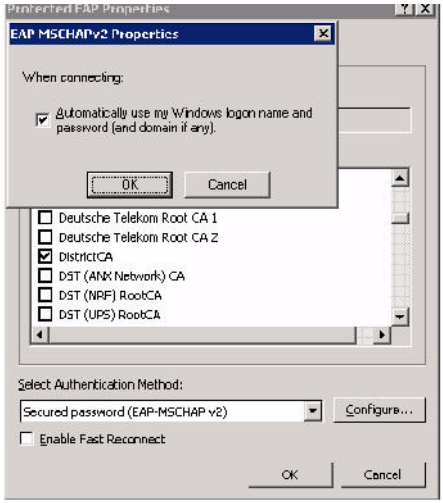
Protected EAP Properties
EAP MSCHAPv2 Properties
When connecting:
Automatically use my Windows logon name and password (and domain if any).
OK
Cancel
Deutsche Telekom Root CA 1
Deutsche Telekom Root CA 2
DistrictCA
DST (ANX Network) CA
DST (NRF) RootCA
DST (UPS) RootCA
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
OK
Cancel

Figure B-6

Appendix C
Internal Captive Portal

You can customize the default captive portal page through the browser interface, as described in Chapter 8, “Configuring the Captive Portal”.You can also create your own web page to display rather than the default page. This appendix discusses creating and installing a new internal captive portal page and other customizations.

It includes the following topics:

Creating a New Internal Web Page

A custom web page must include an authentication form to authenticate a user.

The authentication form can include any of the following variables:

- **user** (Required)
- **password** (Required)
- **FQDN**: The fully qualified domain name.

> **Note:** This is dependent on the setting of the WFS709TP ProSafe Smart Wireless Switch and is supported only by Windows global catalog server software.

The form can use either the “get” or the “post” methods, but the “post” method is recommended. The form’s action must absolutely or relatively reference https://<switch_IP>/auth/index.html/u.

You can construct an authentication form using the following HTML:

```
<FORM method="post" ACTION="/auth/index.html/u">
...
</FORM>
```

A recommended option for the <FORM> element is:

```
autocomplete="off"
```

This tells Internet Explorer not to cache form inputs.

The form variables can be input using any form control method available such as INPUT, SELECT, TEXTAREA and BUTTON. Example HTML code follows.

Username

Minimal:

```
<INPUT type="text" name="user">
```

Recommended Options:

- `accesskey="u"` – Sets the keyboard shortcut to 'u'
- `SIZE="25"` – Sets the size of the input box to 25
- VALUE="" – Ensures no default value

Password

Minimal:

```
<INPUT type="password" name="password">
```

Recommended Options:

- `accesskey = "p"` – Sets the keyboard shortcut to 'p'
- `SIZE = "25"` – the size of the input box to 25
- `VALUE = ""` – Ensures no default value

FQDN

Minimal:

```
<SELECT name=fqdn>
   <OPTION value="fqdn1" SELECTED>
   <OPTION value="fqdn2">
</SELECT>
```

Recommended Options:

None.

You must also include an input button:

```
<INPUT type="submit">
```

Basic HTML Example

```
<HTML>
  <HEAD>
  </HEAD>
  <BODY>
    <FORM method="post" autocomplete="off" ACTION="/auth/index.html/u">

    Username:<BR>
    <INPUT type="text" name="user" accesskey="u" SIZE="25" VALUE="">
    <BR>

    Password:<BR>
    <INPUT type="password" name="password" accesskey="p" SIZE="25"
        VALUE="">
    <BR>

    <INPUT type="submit">
    </FORM>
  </BODY>
</HTML>
```

For a more advanced example, use your browser's View Source function while viewing the default captive portal page.

Installing a New Captive Portal Page

You install the captive portal page by using the Maintenance function of the browser interface.

Log into the browser interface and navigate to Maintenance > Captive Portal > Upload Custom Login Pages. This page lets you upload your own files to the WFS709TP ProSafe Smart Wireless Switch.

There are three page types that you can choose:

- **Captive Portal Login** (top level): This type uploads the file into the WFS709TP ProSafe Smart Wireless Switch and instantly sets the captive portal page to reference the file that you are uploading. Use with caution on a production switch, as this takes effect immediately.
- **Content:** The content page type allows you to upload all miscellaneous files that you need to reference from your main captive portal login page. This can be used for images, CSS files, scripts, or any other file that you need to reference. These files are uploaded into the same directory as the top level-captive portal page, and thus all files can be referenced relatively.

All uploaded files can also be referenced from your top-level captive portal page using any of the following:

- `https://<switch_IP>/upload/<file>`
- `/upload/<file>`
- `<file>`

You can reassign the default captive portal site using the Revert to factory default settings check box in the Upload Custom Login Pages section of the Maintenance tab in the browser interface.

Displaying Authentication Error Message

This section contains a script that performs the following tasks:

- When the user is redirected to the main captive portal login when there is authentication failure, the redirect URL includes a query parameter `errmsg` that JavaScript can extract and display.
- The originally requested URL is stored in a cookie so that once the user has authenticated, they are automatically redirected to their original page.

```
<script>
```

```
{

function createCookie(name,value,days)
{
            if (days)
            {
                        var date = new Date();
                    date.setTime(date.getTime()+(days*24*60*60*1000));
                        var expires = "; expires="+date.toGMTString();
            }
            else var expires = "";
            document.cookie = name+"="+value+expires+"; path=/";
}

  var q = window.location.search;
  var errmsg = null;


  if (q && q.length > 1) {
    q = q.substring(1).split(/[=&]/);
    for (var i = 0; i < q.length - 1; i += 2) {
      if (q[i] == "errmsg") {
        errmsg = unescape(q[i + 1]);
          break;
      }
       if (q[i] == "host") {
          createCookie('url',q[i+1],0)
        }
```

```
    }
  }

  if (errmsg && errmsg.length > 0) {
    errmsg = "<div id='errorbox'>\n" + errmsg + "\n</div>\n";
    document.write(errmsg);
  }
}
</script>
```

Language Customization

The ability to customize the internal captive portal provides you with a very flexible interface to the captive portal system. However, other than posting site-specific messages onto the captive portal website, the most common type of customization is likely to be language localization. This section describes a simple method for creating a native language captive portal implementation using the internal captive portal system.

1. First, customize the page to your liking (see "Personalizing the Captive Portal Page" in Chapter 8). To do this, navigate to the Maintenance > Customize Captive Portal in the browser interface.

   For example, choose a page design, upload a custom logo and/or a custom background. Also include any page text and acceptable use policy that you would like on the page. We recommend that you put this in your target language so it will not need to be translated later.

2. Ensure that Guest login is enabled or disabled, as you prefer. Navigate to Configuration > Authentication Methods > Captive Portal and select or deselect Enable Guest Login, if necessary.

3. Click Submit and then click on View Captive Portal. Check that your customization and text/html is correct, with the default interface still in English and the character set still autodetecting ISO-8859-1.

   Repeat steps 1 through 3 until you are satisfied with your page.

4. Once you have a page you find acceptable, click on View Captive Portal one more time to display your login page. From your browser, choose View->Source or its equivalent. Your system will display the HTML source for the captive portal page. Save this source as a file on your local system.
5. Open the file that you saved using a standard text editor.and make the following changes:
   a. Fix the character set. The default `<HEAD>...</HEAD>` section of the file will look similar to the following:

```
<head>
<title>Portal Login</title>

<link href="default1/styles.css" rel="stylesheet" media="screen"
type="text/css" />
<script language="javascript" type="text/javascript">
   function showPolicy() {
      win = window.open("/auth/acceptableusepolicy.html", "policy",
"height=550,width=550,scrollbars=1");

</script>
</head>
```

   In order to control the character set that the browser will use to show the text with, you will need to insert the following line inside the <HEAD>...</HEAD> element:

```
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS"/>
```

   Replace the Shift_JIS with the character set that is used by your system. In theory, any character encoding that has been registered with IANA can be used, but you must ensure that any text you enter uses this character set and that your target browsers support the required character set encoding.

   The final `<HEAD>...</HEAD>` portion of the document should look similar to this:

```
<head>
<title>Portal Login</title>
```

```
<link href="default1/styles.css" rel="stylesheet" media="screen"
type="text/css" />

<script language="javascript" type="text/javascript">

   function showPolicy() {

      win = window.open("/auth/acceptableusepolicy.html", "policy",
"height=550,width=550,scrollbars=1");

   }

</script>

</head>
```

b. Fix the references: If you have used the built-in preferences, you will need to update the reference for the logo image and the CSS style sheet.

To update the CSS reference, search the text for "`<link href`" and update the reference to include "`/auth/`" in front of the reference. The original link should look similar to the following:

```
<link href="default1/styles.css" rel="stylesheet" media="screen"
type="text/css" />
```

Replace this with a link like the following:

```
<link href="/auth/default1/styles.css" rel="stylesheet" media="screen"
type="text/css" />
```

The easiest way to update the image reference is to search for "`src`" using your text editor and updating the reference to include "`/auth/`" in front of the image file. The original link should look similar to the following:

```
<img src="default1/logo.gif"/>
```

Replace this with a link like this:

```
<img src="/auth/default1/logo.gif"/>
```

c. Insert JavaScript to handle error cases:

When the WFS709TP detects an error situation, it will pass the user's page a variable called *errmsg* with a value of what the error is in English. Currently, only “Authentication Failed” is supported as a valid error message.

To localize the authentication failure message, replace the following text (it is just a few lines below the <body> tag):

```
<div id="errorbox" style="display: none;">
</div>
```

with the script below.

You will need to translate the Authentication Failed error message into your local language and add it into the script below where it states `localized_msg="..."`.

```
<script>
{
  var q = window.location.search;
  var errmsg = null;
  if (q && q.length > 1) {
    q = q.substring(1).split(/[=&]/);
    for (var i = 0; i < q.length - 1; i += 2) {
      if (q[i] == "errmsg") {
        errmsg = unescape(q[i + 1]);
        break;
      }
    }
  }

  if (errmsg && errmsg.length > 0) {
    switch(errmsg) {
    case "Authentication Failed":
    localized_msg="Authentication Failed";
    break;
    default:
      localised_msg=errmsg;
      break;
```

```
    }
    errmsg = "<div id='errorbox'>\n" + localised_msg + "\n</div>\n";
    document.write(errmsg);
  };
}
</script>
```

d. Translate the web page text. Once you have made the changes as above, you only need to translate the rest of the text that appears on the page. The exact text that appears will depend on the WFS709TP settings when you originally viewed the captive portal. You will need to translate all relevant text such as REGISTERED USER, USERNAME, PASSWORD, the `value=""` part of the `INPUT type="submit"` button, and all other text. Ensure that the character set you use to translate into is the same as you have selected in step 5a.

Feel free to edit the HTML as you go if you are familiar with HTML.

6. After saving your changes, upload the file to the WFS709TP using the Maintenance > Upload Custom Login Pages section of the browser interface.

a. Choose Captive Portal Login (top level) and browse your local computer for the file you saved.

b. Ensure that the Revert to factory default settings box is *not* checked and click Apply. This will upload the file to the WFS709TP and set the captive portal system to use this page as the redirection page.

c. To check that your site is operating correctly, go back to the Customize Login page and click View Captive Portal to view the page you have uploaded. Check that your browser has automatically detected the character set and that your text is not garbled.

7. To make any adjustments to your page, edit your file locally and simply re-upload to the WFS709TP in order to view the page again.

8. While it is possible to customize the welcome page on the WFS709TP, for language localization it is recommended that you use an external welcome page instead. This can be a web site on an external server, or it can be a static page that is uploaded to a WFS709TP.

You set the welcome page location in the Configuration > Security > Authentication Methods > Captive Portal page. This is the page that the user will be redirected to after a success authentication.

If you require this to be a page on the WFS709TP, you must create you own web page using the charset meta attribute, and upload this page as “content” to the designated WFS709TP. Any required CSS, Client-side Script files, and media files can also be uploaded, however file space is limited. Check the available space using “show memory” under “flash free” and remember to leave ample room for system files.

Figure C-1 shows a sample of a translated page.

Figure C-1

	Note: The Registered User and Guest User sections of the login page are implemented as graphics files, referenced by the default CSS styles. In order to change these, you will need to create new graphic files, download the CSS file, edit the reference to the graphics files, change the style reference in your index file, and then upload all files as “content” to the WFS709TP.

Customizing the Welcome Page

Once a user has authenticated to the WFS709TP, they are presented with the welcome page. The default welcome page will depend slightly on your configuration, but will look similar to Figure C-2.

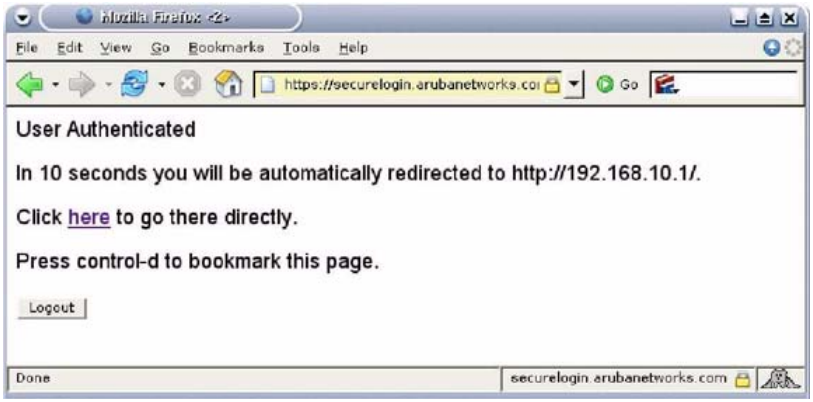

Figure C-2

You can customize this welcome page by building your own HTML page and uploading it to the WFS709TP. You upload it to the WFS709TP using the GUI under Maintenance > Captive Portal > Upload custom pages and choose “content” as the page type. This file is stored under its original name in a directory called /upload/.

In order to actually use this file, you will need to configure the welcome page on the WFS709TP. You can change this via the GUI under Configuration->Authentication Methods->Captive-Portal->Welcome Page Login.

A simple example that will create the same page as Figure C-2 is shown below: The part of the script in red will redirect the user to the web page they originally requested.

```
<html>
<head>
<script>
{

function readCookie(name)
```

```
{
            var nameEQ = name + "=";
            var ca = document.cookie.split(';');
            for(var i=0;i < ca.length;i++)
            {
                        var c = ca[i];
                        while (c.charAt(0)==' ') c =
c.substring(1,c.length);
                        if (c.indexOf(nameEQ) == 0) return
c.substring(nameEQ.length,c.length);
            }
            return null;
}

var cookieval = readCookie('url');
            if (cookieval.length>0) document.write("<meta http-
equiv=\"refresh\" content=\"2;url=http://"+cookieval+"\""+">");



            }
</script>
</head>
<body bgcolor=white text=000000>
<font face="Verdana, Arial, Helvetica, sans-serif" size=+1>
  <b>User Authenticated </b>

<p>In 2 seconds you will be automatically redirected to your original web
page</p>
<p> Press control-d to bookmark this page.</p>

<FORM ACTION="/auth/logout.html">
```

```
      <INPUT type="submit" name="logout" value="Logout">
</FORM>
</font>
</body>
</html>
```

If you customize the welcome page, then you must also customize the pop-up, box if you want to have one.

Customizing the Pop-Up Box

Before you can customize the pop-up box, you must customize your welcome page. Once you have customized your welcome page, then you can configure your custom page to make a pop-up box to enable your users to log themselves out.

The first step is to generate the HTML that will be displayed within the pop-up box. The default HTML is as shown:

```
<html>
<body bgcolor=white text=000000>
<font face="Verdana, Arial, Helvetica, sans-serif" size=+1>
 <b>Logout</b></font>
 <p>
  <a href="/auth/logout.html"> Click to Logout </a>
</body>
</html>
```

If you wish your users to be able to log out using this pop-up box, then you must include a reference to /auth/logout.html. Once a user accesses this URL, the WFS709TP will log them out. It is easiest to simply edit the above HTML to suit your users and then upload the resulting file to the WFS709TP using the GUI under Maintenance > Captive Portal > Upload custom pages and choosing "content" as the page type.

Once you have completed your HTML, then you must get the clients to create the pop-up box once they have logged into the WFS709TP. This is done by inserting the following code into your welcome page text and re-uploading the welcome page text to your WFS709TP. This will let you customize your pop-up window.

```
<script language="JavaScript">
 var url="/upload/popup.html";
 var w=210;
 var h=80;
 var x=window.screen.width - w - 20;
 var y=window.screen.height - h - 60;
 window.open(url, 'logout',
"toolbar=no,location=no,width="+w+",height="+h+",top="+y+",left="+x+",sc
reenX="+x+",screenY="+y);
</script>
```

These are some common elements to change:

- **URL:** Set the URL to be the name of the pop-up HTML file that you created and uploaded. This should be preceded by "/upload/".
- **Width:** Set w to be the required width of the pop-up box.
- **Height**: Set h to be the required height of the pop-up box.
- **Title:** Set the second parameter in the window.open command to be the title of the pop-up box. Be sure to include quotes.

Customizing the Logged Out Box

In order to customize the logged out box, you must first customize your welcome page and also your pop-up box. To customize the message that occurs after you have logged out then you need to replace the URL that the pop-up box will access in order to log out with your own HTML file.

First, you must write the HTML web page that will actually log out the user and will also display the page that you wish. The code for an example page is shown below. The key part that must be included is the `<iframe>..</iframe>` section. This is the part of the HTML that actually does the logout. The logout is always performed by the client accessing the /auth/logout.html file on the WFS709TP and so it is hidden in the HTML page here in order to get the client to access this page and for the WFS709TP to update its authentication status. If a client does not support the iframe tag, then the text between the `<iframe>` and the `</iframe>` is used. This is simply a zero-pixel-sized image file that references /auth/logout.html. Either method should allow the client to log out from the WFS709TP.

Everything else can be customized.

```
<html>
<body bgcolor=white text=000000>


<iframe src='/auth/logout.html' width=0 height=0 frameborder=0><img
src=/auth/logout.html width=0 height=0></iframe>


<P><font face="Verdana, Arial, Helvetica, sans-serif" size=+1>
You have now logged out.</font></P>


<form> <input type="button" onclick="window.close()" name="close"
value="Close Window"></form>


</body>
</html>
```

After writing your own HTML, then you need to ensure that your customized pop-up box will access your new logged-out file. In the pop-up box example above, simply replace “/auth/logout.html” with your own file that you upload to the WFS709TP. For example, if your customized logout HTML is stored in a file called loggedout.html, then your pop-up.html file should reference it like this:

```
<html>
<body bgcolor=white text=000000>
<font face="Verdana, Arial, Helvetica, sans-serif" size=+1>
 <b>Logout</b></font>
 <p>
  <a href="/upload/loggedout.html"> Click to Logout </a>
</body>
</html>
```

Appendix D
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Communications	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing a Computer for Network Access	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Index

Numbers

A

B

C

D

S

T

V

W